الكراس الاحترافي الشامل

في إدارة وتشغيل المصادر البشرية (HUMINT)

الكراس الاحترافي الشامل

في إدارة وتشغيل المصادر البشرية (HUMINT)

منهج تدريبي متكامل للضباط والعاملين في المجال الاستخباراتي

محمد خفي حسن الساعدي

١٤٤٧ هـ. ٢٠٢٥ م

الكراس الاحترافي الشامل

في إدارة وتشغيل المصادر البشرية (HUMINT)

منهج تدريبي متكامل للضباط والعاملين في المجال الاستخباراتي

تأليف: محمد خفي حسن الساعدي

الطبعة: الأولى ١٤٤٧ هـ / ٢٠٢٦ م

المطبعة: دار المناهل

القطع: رقعي

بسم الله الرحمن الرحيم



بِسْمِ اللَّـهِ الرَّحْمَـنِ الرَّحِيمِ

﴿وَلَا تَحْسَبَنَّ الَّذِينَ قُتِلُوا فِي سَبِيلِ اللَّهِ أَمْوَاتًا بَلْ أَحْيَاءٌ عِنْدَ رَبِّهِمْ يُرْزَقُونَ﴾

صدق الله العلي العظيم

(ال عمران الآية ١٦٩)

مقدّمة الكتاب

بِسْمِ اللَّـهِ الرَّحْمَـنِ الرَّحِيمِ

الحمد لله الذي بنعمته تـتم الصـالحات، والصـلاة والسـلام على سيدنا محمد وعلى آل بيته الطاهرين وصحبه أجمعين.

يأتي هذا الكراس ليكون خلاصة جهدٍ بحثي وعلمي رصـين، يهدف إلى توثيق المصادر وتقديم المعرفة بشكل دقيق ومنهجـي، بما يخدم القارئ والباحث ويعزز الـوعي والقـدرة علـى التحليـل واتخاذ القرار. لقد حرصنا في إعداد هذا العمل على اعتماد أفضل الأساليب البحثية، واستناد المعلومات إلى مصادر موثوقة، ليكـون مرجعًا يُعتدّ به ومساهمة متواضعة في مسـيرة المعرفـة الوطنيـة إن خدمة الوطن شرف، وإتقان العمل مسـؤولية، والارتقـاء بالمعرفـة واجب لا يقل أهمية عن الواجبات العسكرية والأمنية. ومـن هـذا المنطلق، تم إعداد هذا الكراس بعنايـة ليكـون عامـل دعـم لكـل جهد يسهم في تعزيز أمن البلاد واستقرارها، وإسناد العاملين فـي

الميدان بالمعرفة التي ترفع من مستوى الأداء والدقة. نسأل الله أن يجعل هذا العمل خالصًا لوجهه، نافعًا لكل من يقرأه، وسندًا للعاملين بإخلاص من أجل حماية وطننا العزيز العراق بلاد الرافدين

اعداد المقاتل

محمد خفي حسن الساعدي (الملقب أبو علي الساعدي)

اهدي ثواب هذا العمل الى أرواح الشهداء السعداء

التاريخ المصادف ٢٧ / ١١ / ٢٠٢٥

إهداء

«شهداؤنا قادتنا الرحمة والخلود للشهداء الابطال»

بِسْمِ اللَّـهِ الرَّحْمَـنِ الرَّحِيمِ

﴿وَلَا تَحْسَبَنَّ الَّذِينَ قُتِلُوا فِي سَبِيلِ اللَّهِ أَمْوَاتًا بَلْ
أَحْيَاءٌ عِنْدَ رَبِّهِمْ يُرْزَقُونَ * فَرِحِينَ بِمَا آتَاهُمُ اللَّهُ مِنْ
فَضْلِهِ وَيَسْتَبْشِرُونَ بِالَّذِينَ لَمْ يَلْحَقُوا بِهِمْ مِنْ خَلْفِهِمْ
أَلَّا خَوْفٌ عَلَيْهِمْ وَلَا هُمْ يَحْزَنُونَ﴾

(صدق الله العلي العظيم)

(سورة آل عمران ـ الآية ١٦٩-١٧٠)

إهداء

إلى شهدائنا الأبرار شهداء الحشد الشعبي وشهداء القوات الأمنية وشهداء القوات المسلحة وشهداء المقاومة البطلة الذين قدّموا أرواحهم الطاهرة فداءً للوطن، فكانوا مناراتٍ تهدي طريقنا، ورمز التضحية والبطولة التي لا تُنسى. وإلى جميع التشكيلات والمؤسسات الأمنية التي وقفت وما زالت تقف سدًّا منيعًا أمام كل تهديد يمس أمن العراق واستقراره. لكم كل الوفاء والعرفان. وإلى أبناء وطننا الغيارى رجالا ونساء والى أبناء العشائر والمواكب الحسينية الذين مدّوا يد العون، وساندوا، ووقفوا مع رجالهم في الميدان بالكلمة، والدعم، والموقف، والجهد... فكانوا شريكًا أصيلًا في كل نجاح وإنجاز.إلى كل هؤلاء... نهدي هذا العمل، وفاءً وتقديرًا، وإيمانًا بأن الوطن يُبنى بسواعد أبنائه وبدماء شهدائه وبعطاء المخلصين فيه.

المقدمة العامة

يمثل هذا الكـراس نموذجـاً تـدريبيًا حـديثًا ومتكـاملاً فـي إدارة وتشــغيل المصــادر البشــرية (HUMINT)، ويســتهدف الضــباط والمنتسبين العاملين في المجالات العملياتية والاستخباراتية والأمنية.

يهدف الكراس إلى:

١. تطوير مهارات تشغيل المصادر بطريقة علمية واحترافية

٢. تزويد الضباط بأحدث الأساليب التشغيلية والاستخباراتية

٣. دمـج التقنيـات الحديثـة (Cyber–HUMINT) ، التحليـل البيومتري، (الأمن الرقمي)

٤. تقديم أمثلة موسعة وورش عملية لتطبيق المعرفـة مباشـرة في الميدان

يجمع الكراس بين الدورات النظرية، الأمثلة الواقعية، الورش التطبيقية، سيناريوهات التشـغيل، النمـاذج العمليـة، والفهرسـت المتكامل ليكون مرجعًا شاملاً في المجال.

الفصل الأول

مدخل إلى عالم المصادر (أساسي)

١. مفهوم المصدر الاستخباراتي

الشرح:

المصدر الاستخباراتي هو الفرد أو الجهة التي توفر معلومات دقيقة وحساسة لدعم اتخاذ القرار الأمني والاستخباراتي. يُعتبر المصدر الركيزة الأساسية لأي منظومةHUMINT حيث توفر المصادر البشرية بيانات نوعية لا تستطيع الوسائل التقنية وحدها جمعها.

المفهوم:

فهم طبيعة المصدر يساعد الضابط على:

اختيار طريقة التعامل الأمثل.

تحديد مستوى الثقة والمخاطر المرتبطة بالمصدر.

وضع استراتيجيات التجنيد والتحفيز الملائمة.

سيناريو عملي:

مقابلة شخصية مع موظف في مؤسسة حساسة بهدف تقييم إمكانية الحصول على معلومات حول مشروع داخلي. يتم تقييم استجابته، معرفته بالمخاطر، ودرجة انفتاحه على التعاون.

٢. أهمية المصادر في العمل الأمني

الشرح:

المصادر تمثل العمود الفقري لجمع المعلومات النوعية في البيئات المعقدة. فهي تكمل التقنيات الإلكترونية والاستطلاعات الفنية، وتتيح الحصول على معلومات سرية أو داخلية لا يمكن رصدها عن بعد.

المفهوم:

بدون مصادر بشرية موثوقة، أي نظام استخباراتي سيواجه قصورًا في المعلومات النوعية.

المصادر تمكن الضابط من اتخاذ قرارات دقيقة وتقليل المخاطر التشغيلية.

سيناريو عملي:

وجود مصدر داخل مؤسسة منافسة يساعد على معرفة نواياها بدون الاعتماد على اختراقات إلكترونية.

٣. تصنيفات المصادر

الشرح:

تصنيف المصادر يتم بناءً على الدافع والبيئة التي يعمل بها المصدر، وتشمل:

مصادر صديقة: أشخاص مستعدين للتعاون بسبب الثقة أو العلاقة الشخصية.

مصادر انتهازية: يبحثون عن مكاسب شخصية مادية أو معنوية.

مصادر حساسة داخل مؤسسة: لديهم وصول لمعلومات حساسة ويحتاجون للتجنيد بحذر شديد.

مصادر ضمن جماعات معادية: أشخاص يعملون داخل كيانات معادية ويحتاجون لإدارة مخاطر عالية.

المفهوم:

كل تصنيف يتطلب استراتيجية مختلفة للتجنيد والتحفيز والحماية.

اختيار أسلوب الاقتراب والتواصل يتأثر بنوع المصدر وتصنيفه.

سيناريو عملي:

مصدر انتهازي داخل مؤسسة حكومية: الضابط يصمم خطة تشمل مكافآت معنوية ومادية مع مراقبة دقيقة لتجنب المخاطر.

٤. المهارات الأساسية للضابط في التعامل مع المصادر

الشرح:

الضابط يجب أن يمتلك مهارات أساسية لضمان تشغيل المصادر بكفاءة:

مهارات التحليل النفسي: فهم دوافع المصدر وسلوكه المتوقع.

مهارات الاتصال الفعال: استخدام لغة واضحة، وضبط نبرة الصوت، والإشارات غير اللفظية.

مهارات تقييم المخاطر: القدرة على تقدير احتمالية الخداع أو تسريب المعلومات.

المفهوم:

تطوير هذه المهارات يُمكّن الضابط من تحقيق أقصى إنتاجية للمصدر مع أدنى مخاطر تشغيلية.

سيناريو عملي:

مقابلة تقييمية لمصدر جديد، يقوم الضابط بتسجيل لغة جسده، صمته، ردود فعله، ومدى استعداده للتعاون مع توقع النتائج المحتملة.

٥. أدوات ومواد مطلوبة

دفتر ملاحظات لتوثيق الانطباعات والسلوك.

استمارة تقييم أولية للمصدر (تحتوي على مؤشرات: الثقة، الاستجابة، الدوافع، المعرفة بالمجال).

سيناريوهات تمثيل أدوار لتدريب الضباط على مختلف تصنيفات المصادر.

٦. التمارين العملية

تقييم مصدر افتراضي: يتم تقديم وصف لشخصية هدف، ويطلب من الضابط تحديد مستوى الولاء، القدرة، الاستقرار، ومخاطر التعامل.

محاكاة مقابلة: يقوم الضابط بإجراء مقابلة قصيرة لمدة ١٠ دقائق مع مصدر افتراضي، مع التركيز على ملاحظة المؤشرات السلوكية والنفسية.

تصنيف المصادر: تقديم مجموعة من الشخصيات المختلفة، وعلى المتدرب تصنيفها وتحديد استراتيجية الاقتراب المناسبة لكل واحدة.

٧. مخرجات التعلم المتوقعة

فهم شامل لمفهوم المصادر وأهميتها في HUMINT.

القدرة على تصنيف المصادر بدقة بناءً على الدافع والبيئة.

القدرة على استخدام أدوات التقييم الأولية لتقـدير المخـاطر والولاء.

تطوير خطة أولية للتعامل مع أي مصدر.

الفصل الثاني
السمات النفسية والسلوكية للمصادر (أساسي)

١. السمات النفسية الأساسية

الشرح

الصفات الفكرية والعاطفية للمصدر تحدد طريقة استجابته للتوجيهات، سرعة تعلمه، والتزامه بالتعليمات. تشمل هذه الصفات:

١. القدرة على التحليل والتفكير المنطقي.

٢. التحكم العاطفي عند مواجهة ضغوط أو تهديدات.

٢. القدرة على اتخاذ القرار الفردي أو الاستجابة للأوامر.

المفهوم

١. فهم هذه السمات يمكّن الضابط من اختيار أسلوب

الاقتراب والتوجيه والتحفيز الأمثل لكل مصدر.

٢. تقييم السمات النفسية يساعد في تحديد المخاطر واحتمالية استقرار العلاقة مع المصدر.

سيناريو عملي:

١. تقييم مصدر جديد من خلال مقابلة قصيرة، يراقب فيها الضابط ردود الفعل العاطفية، مستوى التركيز، ومرونة التفكير عند طرح أسئلة غير متوقعة.

٢. المؤشرات السلوكية

الشرح

لغة الجسد، نبرة الصوت، توقيت الرد، وحركات العين تُظهر صدق المصدر أو محاولة التضليل.

١. التوتر يظهر في حركات غير إرادية (مثل لمس الوجه أو اللعب بالأصابع).

٢.التردد في الرد يشير إلى عدم اليقين أو محاولة الالتفاف.

٣.التناقض بين الكلام والسلوك يشير إلى احتمالية الكذب أو التحفظ.

المفهوم:

١. استخدام المؤشرات السلوكية يتيح للضابط كشف الخداع مبكرًا واتخاذ إجراءات متابعة أو اختبار إضافية.

سيناريو عملي

١. مقابلة مصدر، مع تسجيل كل التغيرات السلوكية مقابل كل سؤال، ثم تحليل هذه الملاحظات لتحديد مستوى صدقه.

٣. فهم الدوافع

الشرح:

الدوافع الداخلية والخارجية للمصدر تحدد مدى التزامه وتفاعله. تشمل الدوافع:

١. مالية: مكافآت مادية أو فوائد ملموسة.

٢. أيديولوجية: القناعات السياسية أو الدينية.

٣. خوف أو ضغوط: تهديدات محتملة قد تدفع المصدر للتعاون أو للتراجع.

٤. طموح شخصي: رغبة في الحصول على امتيازات مهنية أو اجتماعية.

المفهوم

١. معرفة دوافع المصدر يسمح للضابط بتصميم أسلوب تحفيزي مناسب وزيادة الالتزام.

٢. توازن الدافع الخارجي مع الداخلي يحقق استدامة المعلومات وتحسين جودة التقارير.

سيناريو عملي:

١. التعامل مع مصدر لديه دوافع مالية فقط: تصميم خطة تحفيزية تعتمد على مكافآت مالية دورية، مع متابعة الالتزام بالمعلومات المقدمة.

٤. أدوات ومواد مطلوبة

استمارة تحليل نفسي وسلوكي: لتقييم كل محور (القدرة الذهنية، التحكم العاطفي، الدافع، السلوك).

فيديوهات وملاحظات تمثيلية: لمشاهد تحليل لغة جسد وسلوك.

أدوات تسجيل الملاحظات: دفتر أو نظام رقمي لتوثيق المؤشرات السلوكية أثناء اللقاءات.

٥. التمارين العملية

١. تحليل سلوكي لمصدر افتراضي: تقديم حالة مصدر وتسجيل كافة المؤشرات السلوكية والنفسية المحتملة، ثم كتابة تقرير تحليلي.

٢. محاكاة مقابلة: ضابط يقوم بإجراء مقابلة لمدة ١٥ دقيقة، ويركز على رصد المؤشرات السلوكية والتغيرات العاطفية للمصدر.

٣. مهمة تقييم دوافع: تقديم سيناريوهات مختلفة، وعلى الضابط تحديد الدافع المحتمل لكل مصدر ووضع خطة تحفيزية مبدئية.

٦. مخرجات التعلم المتوقعة

١. القدرة على تحديد السمات النفسية الأساسية للمصدر.

٢. معرفة المؤشرات السلوكية الدقيقة التي تساعد في كشف الخداع.

٣. القدرة على تقدير دوافع المصدر وتصميم تحفيز مناسب.

كتابة تقرير تحليلي شامل عن المصدر يغطي السمات النفسية والسلوكية والدوافع.

الفصل الثالث

دورة حياة المصدر (أساسي)

١. البحث المسبق

الشرح:

قبل الاقتراب من أي هـدف، يجـب دراسـة خلفيـة المصـدر لتقليل المخاطر التشغيلية. يشمل ذلك:

١. المعلومات المهنية: الوظيفة، المسؤوليات، مدى الوصـول للمعلومات.

٢.الخلفية الشخصية: العائلة، الأصدقاء، علاقات سـابقة مـع مؤسسات أمنية أو استخباراتية.

٣. السمات النفسية والسلوكية الأساسية

المفهوم:

١. معرفة البيئة المهنية والشخصية للمصـدر تمكّـن الضـابط من وضع خطة تشغيل آمنة

٢.البحث المسبق يقلّل مفاجآت العملية ويزيد من احتمالية نجاح التجنيد.

سيناريو عملي:

١. تقييم مصدر محتمل داخل مؤسسة حكومية: جمع معلومات مفتوحة المصدر، مراجعة سجلات عامة، تحليل شبكة علاقاته.

٢. الاقتراب الأول

الشرح:

اللقاء الأول مع الهدف لتقييم رد فعله وإمكانية بناء الثقة.

١. استخدام أسلوب ودّي أو مهني بدون ضغط.

٢. اختبار تجاوب المصدر مع الأسئلة البسيطة وغير الحساسة.

٣. رصد الانطباع الأول، درجة الفضول، والتحفظ.

المفهوم:

١. خطوة أساسية لتحديد إمكانية التعاون المستقبلي.

٢. تقييم مدى ملاءمة المصدر للاستثمار على المدى الطويل.

سيناريو عملي:

١. لقاء ١٠ دقائق مع مصدر محتمل: الضابط يسجل ردود الفعل، ويقدّر مستوى التفاعل والتعاون المتوقع.

٣. بناء الثقة الأساسية

الشرح:

تطوير علاقة تدريجية ومستقرة مع المصدر لضمان التزامه بالمعلومات المقدمة.

١. الاتساق في التعامل والالتزام بالوعود.

٢. احترام الخصوصية والسرية.

٣. منح امتيازات صغيرة (micro-rewards) لتعزيز العلاقة.

المفهوم:

١. الثقة المفتاحية لضمان إنتاجية عالية ومستدامة للمعلومات

سيناريو عملي:

١ بدء تشغيل مصدر بمهمة بسيطة: تقديم طلب معلومات عامة ومتابعة الالتزام بالمواعيد وجودة المعلومات.

٤. التشغيل البسيط

الشرح:

إعطاء المصدر مهمة أولية غير حساسة لاختبار مستوى الالتزام:

١. طلب معلومات عامة أو سهلة التحقق.

٢. متابعة دقة المعلومات وسرعة الاستجابة.

٣. تسجيل الملاحظات حول السلوك أثناء التنفيذ.

المفهوم:

١. يتيح تقييم التزام المصدر قبل منح مهام أكثر حساسية.

٢. يقلّل المخاطر التشغيلية المبكرة ويضع أسسًا لتوسيع نطاق التعاون.

سيناريو عملي:

١. تكليف المصدر بتقديم تقرير أسبوعي عن نشاطات عامة داخل المؤسسة، مع مراقبة جودة التفاصيل ودقة المواعيد.

٥. التقييم المستمر

الشرح:

متابعة جودة المعلومات المقدمة واستمرار الالتزام بالبروتوكولات.

١. مراجعة المعلومات بشكل دوري.

٢. تقييم أي تغييرات في السلوك أو الدوافع.

٣. تحديد نقاط ضعف محتملة واتخاذ إجراءات تصحيحية.

المفهوم:

١. يقلل المخاطر ويضمن استمرار العملية بشكل آمن وفعال.

٢. التقييم المستمر يتيح التكيف مع أي تغييرات في ظروف المصدر.

سيناريو عملي

١. إجراء تقييم كل شهر لمصدر نشط: مراجعة تقارير، مقارنة المؤشرات مع الأداء السابق، تحديث خطة التشغيل الفردية.

٦. أدوات ومواد مطلوبة

١. استمارات متابعة دورة حياة المصدر.(PDF/Word)

٢. قوائم تدقيق لمراحل التشغيل (Checklists) لكل مرحلة.

٣. سجلات ملاحظات وتحليل الأداء للمصادر.

٧. التمارين العملية

١. مهمة البحث المسبق: تقديم ملف مصدر افتراضي، مع جمع وتحليل المعلومات لتحديد مخاطر الاقتراب.

٢. محاكاة الاقتراب الأول: لعب دور الضابط والمصدر لتقييم التفاعل وردود الفعل.

٣. بناء الثقة والتشغيل البسيط: تصميم خطة لمصدر جديد تشمل مهمة أولية، طريقة تحفيز، وسجل متابعة.

٤. تقييم مستمر: مراجعة تقرير شهري لمصدر وتقديم توصية تشغيلية لتعديل الخطة.

٨. مخرجات التعلم المتوقعة

١. القدرة على إجراء بحث مسبق شامل لتقليل المخاطر.

٢. مهارة تنفيذ الاقتراب الأول وبناء الثقة بطريقة احترافية.

٣. إدارة تشغيل المصدر البسيط والتقييم المستمر لضمان جودة المعلومات.

٤. كتابة تقرير متكامل عن دورة حياة المصدر يشمل كل المراحل والملاحظات والتوصيات.

الفصل الرابع

مبادئ الأمن التشغيلي الأساسي (أساسي)

١. أمن الضابط

الشرح:

حماية الضابط نفسه هي الخطوة الأولى لضمان نجاح أي عملية استخباراتية. يشمل ذلك:

١. الحفاظ على سرية الهوية والموقع والمهام.

٢. استخدام خطوط اتصال آمنة ومشفرة عند التعامل مع المصادر.

٣. التحرك بطريقة غير ملفتة للانتباه داخل بيئات حساسة.

٤. توخي الحذر في الأماكن العامة والرقمية، بما في ذلك شبكات الإنترنت والاجتماعات.

المفهوم:

١. حماية الضابط مباشرة تؤدي إلى حماية العملية والمصدر.

٢. أي اختراق أو تسريب يمكن أن يؤدي إلى فقدان الثقة أو كشف الشبكة.

سيناريو عملي:

١. عند زيارة مصدر داخل مؤسسة، يخطط الضابط للمكان والوقت بعناية، يختار طرق وصول متنوعة، ويحرص على عدم رصد خطواته عبر كاميرات المراقبة.

٢. أمن المصدر

الشرح :

١. توعية المصدر بكيفية حماية نفسه أثناء جمع وتقديم المعلومات.

٢. تعليم المصدر استخدام وسائط اتصال مشفرة أو آمنة.

٣. تجنب كشف المصدر لأي طرف ثالث أو بيئة قد تكون معادية.

٤. مراقبة سلوك المصدر لتفادي أي تهديدات محتملة على حياته أو وظيفته.

المفهوم :

١. مصدر آمن يعني معلومات أكثر موثوقية واستمرارية العملية.

٢. تقليل المخاطر على المصدر يعزز الالتزام ويزيد الإنتاجية الاستخباراتية.

سيناريو عملي :

١. تزويد مصدر داخل مؤسسة حكومية بهاتف مشفر وإرشاد حول أوقات وأماكن إرسال المعلومات بحيث يقلل التعرض للمراقبة.

٣. إدارة المخاطر الأولية

الشرح

١. تحديد التهديدات المحتملة قبل وأثناء العملية.

٢. وضع خطط بديلة للطوارئ (Plan B و Plan C).

٣. تقييم نقاط الضعف في المصدر، الضابط، وبيئة التشغيل.

٤. استخدام أساليب بسيطة لمراقبة الأخطار: مراقبة كاميرات، استخدام تغطية اجتماعية، مراجعة مؤشرات التهديدات.

المفهوم :

١. يضمن استمرارية العمليات وتقليل الخطر على جميع الأطراف.

٢. تقليل المخاطر المبكرة يمنع حدوث كوارث تشغيلية أو كشف الشبكة.

سيناريو عملي :

١. قبل لقاء المصدر، يقوم الضابط بتحليل موقع اللقاء: نقاط

دخول وخروج آمنة، مراقبة محتملة مـن جهـات خارجيـة، وجـود سيارات أو كاميرات يمكن أن تكتشف اللقاء.

٢. وضع سيناريو احتياطي لنقل المصدر أو تغيير مكان اللقاء إذا ظهرت تهديدات.

٤. أدوات الأمن التشغيلي

وسائل تشـفير الاتصـالات: هواتـف مشـفرة، بـرامج رسـائل مؤمنة، استخدام VPN

التغطيـة والتشـويش: اسـتخدام سـيارات مختلفـة، تغييـر الملابس، استخدام عناوين مختلفة للتواصل.

سـجلات الأمـان: تسـجيل أي نشـاط غيـر معتـاد أو تهديـد محتمل.

التحليـل المسـتمر للمخـاطر: متابعـة الأحـداث المحيطـة وتحديث الإجراءات التشغيلية وفقًا لذلك.

٥. التمارين العملية

١. محاكاة أمن الضابط: تدريب على التحرك في بيئة مكتظـة بدون كشف الهوية أو الهدف.

٢. أمن المصدر: توجيه مصدر افتراضي حول كيفية حماية نفسه وإرسال المعلومات بأمان.

٣. تقييم المخاطر الأولية: تحليل موقع لقاء عملي، وضع سيناريوهات بديلة للتعامل مع أي تهديد.

٤. تدريب تشفير الاتصالات: خطوط اتصال مشفرة واختبار مقاومتها للاختراق.

٦. المخرجات المتوقعة

١. القدرة على حماية الضابط والمصدر بشكل فعال.

٢. معرفة كيفية إدارة المخاطر الأولية ووضع خطط طوارئ فعالة.

٣. تطوير مهارات التخطيط والتقييم الأمني للعمليات البسيطة والمعقدة.

٤. فهم كامل لأدوات وتقنيات الأمن التشغيلي الأساسي لاستخدامها في أي بيئة.

لفصل الخامس

التقييم الأولي واختيار الهدف

١. خصائص الهدف المناسب

الشرح:

يجب أن يمتلك الهدف وصولًا للمعلومة المطلوبة وقابلية للتعاون.

تقييم مدى تأثيره في المؤسسة أو البيئة التي يعمل بها.

القدرة على تقديم معلومات دقيقة وموثوقة.

إمكانية التعاطي مع أساليب التحفيز المختلفة دون ضغط أو إجبار.

المفهوم:

اختيار الهدف الصحيح يقلل المخاطر ويزيد من كفاءة العملية الاستخباراتية.

تقييم الهدف هو الخطوة الأولى لضمان نجاح التجنيد أو تشغيل المصدر.

سيناريو عملي:

ضابط يرصد موظفًا داخل مؤسسة حكومية يمتلك صلاحيات الوصول إلى مستندات حساسة، يقوم بتحليل سلوكه، علاقاته، ونقاط ضعفه قبل الاقتراب منه.

٢. نموذج ٤ Aالأساسي

الشرح:

نموذج مبسط لتقييم الهدف يعتمد على أربعة محاور رئيسية:

الولاء (Allegiance) : درجة ولاء الهدف لأفكاره أو مؤسسته، واستعداده للتعاون.

القدرة (Ability) : إمكانية الوصول إلى المعلومات المطلوبة، ومهاراته التقنية أو الإدارية.

الوصول: (Access) : مستوى وصول الهدف للمعلومات الحساسة والسرية.

الاستقرار (Stability) : الثبات النفسي والسلوكي، مستوى الضغوط، واحتمالية التغير المفاجئ في الموقف.

المفهوم:

تقييم الهدف وفق هذا النموذج يمكّن الضابط من وضع خطة تشغيلية دقيقة.

كل محور من المحاور الأربعة يمكن قياسه باستخدام مؤشرات معيارية قبل الاقتراب.

سيناريو عملي:

تحليل موظف في مؤسسة مالية: الولاء متوسط، القدرة عالية، الوصول محدود، الاستقرار جيد. بناءً على ذلك، يصمم الضابط استراتيجية تجنيد تدريجية مع متابعة دقيقة.

٣. التقييم البيئي

الشرح:

دراسة البيئة الاجتماعية والمهنية للهدف قبل الاقتراب.

فهم علاقاته مع زملائه، مرؤوسيه، وعلاقاته الشخصية.

تقييم أي تهديدات محتملة، مثل رقابة مؤسسية أو تأثير جماعات خارجية.

المفهوم:

فهم البيئة المحيطة بالهدف يقلل المفاجآت ويزيد من فرص نجاح عملية الاقتراب أو التجنيد.

يشمل التقييم البيئي جمع معلومات من مصادر مفتوحة (Open-Source) وتحليل العلاقات والشبكات المحيطة بالهدف.

سيناريو عملي:

قبل مقابلة موظف حساس، يقوم الضابط بتحليل تحركاته اليومية، جدول اجتماعاته، وبيئة مكتبه لتحديد أفضل وقت ومكان للقاء الأول.

٤. أدوات التقييم الأولي

قوائم التحقق A٤ : لتقييم الولاء، القدرة، الوصول، والاستقرار لكل هدف.

نماذج جمع المعلومات البيئية: ملفات خلفية، سجلات عامة، شبكات علاقات.

مؤشرات الأداء الأولي: مستوى الالتزام، دقة المعلومات، قابلية التعاون.

خرائط التهديد: لتحديد المخاطر المحتملة أثناء الاقتراب أو التشغيل.

٥. التمارين العملية

تحليل هدف افتراضي: تقييم موظف باستخدام نموذج A٤ مع تحديد نقاط القوة والضعف.

إعداد خريطة بيئية: إنشاء ملف يوضح البيئة الاجتماعية والمهنية للهدف، مع مؤشرات المخاطر.

محاكاة أول لقاء: اختبار ردود فعل الهدف على أساليب الاقتراب الأولية.

تمرين دمج البيانات: تحويل المعلومات البيئية إلى خطة تشغيلية مبسطة.

٦. المخرجات المتوقعة

القدرة على اختيار الأهداف المناسبة وفق معايير A٤ .

فهم البيئة المحيطة بالهدف وتحديد المخاطر بدقة.

وضع خطة تشغيلية أولية مع مؤشرات نجاح واضحه.

الفصل السادس

بناء العلاقة ومرحلة الاقتراب

١. قواعد الثقة الأساسية

الشرح :

١. الاتساق: يجب أن تكون تصرفات الضابط متناسقة مع كلماته لتقوية المصداقية.

٢. الاحترام: معاملة الهدف باحترام دون التقليل من قيمته.

٣. السرية: الحفاظ على المعلومات المشتركة وعدم تسريب أي تفاصيل خارج الإطار الرسمي.

المفهوم:

١. الثقة هي أساس أي علاقة طويلة الأمد مع المصدر.

٢. بدون ثقة، أي معلومات يتم جمعها قد تكون مغلوطة أو غير مكتملة.

سيناريو عملي :

١. ضابط يتعامل مع موظف في مؤسسة حساسة: يحرص على الالتزام بالمواعيد، عدم الضغط على الهدف، وتوثيق جميع اللقاءات لضمان شعور الهدف بالأمان والثقة.

٢. أساليب الاقتراب الأولية

الشرح :

١. اجتماعي: استخدام فرص اللقاءات غير الرسمية، مثل مناسبات مشتركة أو نشاطات مهنية.

٢. مهني: بناء علاقة عمل مشتركة، مثل طلب مشورة أو مشاركة مشروع، مع مراعاة السرية وعدم الكشف عن الهدف الفعلي المباشر.

٣. تدريجي: تقديم المعلومات والطلبات بشكل متدرج لتجنب شعور الهدف بالضغط.

المفهوم

١. الاقتراب التدريجي يقلل المخاطر ويزيد احتمال قبول الهدف للتعاون.

٢. اختيار الأسلوب المناسب يعتمد على نوع المصدر وبيئته ونقاط ضعفه.

سيناريو عملي :

١. موظف جديد في مؤسسة أمنية: ضابط يبدأ بالتواصل عبر البريد الرسمي لطلب استشارة فنية، ثم تدريجيًا يقدم طلبات معلومات بسيطة، مع مراقبة التزام المصدر واستجابته.

٣. أخطاء الاقتراب الشائعة

الشرح :

١. الإفراط في الضغط: دفع الهدف لتقديم معلومات أكثر من قدرته أو استعداده.

٢. كشف النية: إظهار الهدف النهائي من اللقاء قبل الوقت المناسب.

٣. تقديم وعود مبالغ فيها: أي وعود غير قابلة للتحقق أو الالتزام بها تقلل الثقة.

المفهوم :

١. تجنب هذه الأخطاء يضمن استمرار العلاقة على المدى الطويل ويقلل من احتمال كشف العملية.

سيناريو عملي :

١. ضابط يحاول تحفيز موظف لتقديم معلومات سرية: إذا ضغط بشكل كبير أو وعد بمكافآت غير واقعية، قد يتراجع الهدف أو ينكشف الأمر للمؤسسة.

٤. أدوات وتقنيات بناء العلاقة

١. قوائم متابعة اللقاءات: توثيق كل لقاء، ما تم مناقشته، وسلوك الهدف.

٢. تمارين محاكاة: تدريب الضباط على إدارة اللقاءات الأولية بشكل آمن.

٣. تقنيات التحفيز التدريجي: تقديم مهام صغيرة قابلة للتحقيق لزيادة التفاعل والثقة.

٤. تقييم المخاطر: تحليل احتمالية رفض الهدف أو كشف النوايا.

٥. التمارين العملية

١. محاكاة لقاء أول: الضابط يجري مقابلة لمدة ٢٠ دقيقة مع هدف افتراضي، مع تسجيل ردود الفعل ومؤشرات الثقة.

٢. تمرين تدريجي على طلب المعلومات: تقديم طلبات بسيطة ومتزايدة التعقيد لمعرفة استجابة المصدر.

٣. ورشة الأخطاء الشائعة: تحليل سيناريوهات سابقة واستخلاص الدروس لتجنب الأخطاء في المستقبل.

٦. المخرجات المتوقعة

١. القدرة على بناء علاقة أولية آمنة وفعّالة مع الهدف.

٢. معرفة الأساليب المناسبة للاقترب التدريجي والتواصل.

٣. تحديد نقاط القوة والضعف في استجابة المصدر.

٤. إعداد خطة متابعة أولية قبل الانتقال إلى مرحلة التشغيل أو جمع المعلومات الحساسة.

الفصل السابع

مهارات المقابلة التشغيلية الأساسية

١. تخطيط المقابلة

الشرح :

١. تحديد الأهداف: معرفة نوع المعلومات المطلوبة من اللقاء.

٢. اختيار المكان المناسب : مكان آمن، بعيد عن المراقبة أو الانتباه العام.

٣. توقيت اللقاء: اختيار وقت مناسب للطرفين لتقليل التوتر وزيادة الاستجابة.

٤. إعداد الأسئلة: صياغة أسئلة واضحة، متدرجة بين المفتوحة والمغلقة حسب الهدف.

المفهوم :

١. التخطيط الجيد يضمن جمع معلومات دقيقة وموثوقة، ويقلل من المخاطر التشغيلية.

سيناريو عملي

ضابط يحتاج معرفة رأي موظف في مشروع حساس: يختار مكتبًا هادئًا بعد الدوام الرسمي، يجهز ٥ أسئلة مفتوحة حول المشكلات العامة أولًا قبل الانتقال للمعلومات الحساسة.

٢. إدارة الحوار

الشرح :

١. التحكم في مجرى الحديث دون الضغط على الهدف.

٢. استخدام الاستماع النشط : إعادة صياغة ما يقوله المصدر للتأكد من الفهم.

٣. توجيه الحوار بشكل غير مباشر للحصول على المعلومات المطلوبة تدريجيًا.

٤. الحفاظ على التواصل البصري والإشارات غير اللفظية لتعزيز الثقة.

المفهوم :

١. إدارة الحوار بشكل فعّال تزيد من فرص الحصول على معلومات دقيقة وتقلل من مقاومة المصدر.

سيناريو عملي :

خلال لقاء، يبدأ المصدر بسرد معلومات عامة، والضابط

يستخدم أسئلة استكشافية لتوجيه الحديث تدريجيًا نحو نقاط حساسة دون إثارة القلق أو الشك.

٣. علامات الخداع المبسطة

الشرح :

١. ملاحظة تناقضات السلوك : اختلاف لغة الجسد عن الكلام.

٢. مراقبة نبرة الصوت: التردد أو التغيير المفاجئ قد يشير للكذب.

٣. متابعة توقيت الردود : بطء أو تعجيل غير معتاد.

٤. الانتباه للحركات الصغيرة: العينين، اليدين، القدمين.

المفهوم :

١. مراقبة العلامات السلوكية تساعد الضابط على تمييز المعلومات الصحيحة من المغلوطة في الوقت الحقيقي.

سيناريو عملي :

١. المصدر يتحدث بثقة عن مهمة غير حساسة، لكنه يتجنب النظر مباشرة، أو يغير نبرة صوته عند ذكر تفاصيل حساسة، مما يشير إلى احتمالية عدم الصدق.

٤. أدوات وتقنيات المقابلة

١. قوائم الأسئلة القياسية: تشمل أسئلة استكشافية، أسئلة اختبار، وأسئلة تحفيزية.

٢. لوحة إشارات غير لفظية: لملاحظة ردود فعل المصدر خلال الحديث.

٣. سجل الملاحظات: التوثيق كل إجابة ومؤشر سلوكي أثناء اللقاء.

٤. تقنيات إعادة التوجيه: إعادة صياغة السؤال بطريقة مختلفة لتأكيد صحة الإجابة.

٥. التمارين العملية

١. محاكاة مقابلة أولية: مدة ١٥-٢٠ دقيقة مع هدف افتراضي، تسجيل جميع الملاحظات السلوكية.

٢. تمرين التعرف على علامات الخداع: عرض فيديو لمقابلة وتحليل ١٠ مؤشرات سلوكية.

٣. ورشة إعادة صياغة الأسئلة: تحويل سؤال مغلق إلى سؤال مفتوح للحصول على معلومات أكثر.

٦. المخرجات المتوقعة

١. القدرة على تخطيط وإدارة مقابلة تشغيلية بشكل آمن وفعّال.

٢. التمييز بين علامات الصدق والخداع البسيطة.

٣. استخدام أدوات ومؤشرات عملية لتحليل استجابة المصدر في الوقت الحقيقي.

٤. إعداد تقرير مقابلة أولية يربط المعلومات بالمؤشرات السلوكية.

الفصل الثامن

إدارة وتشغيل المصادر الأساسية

١. إعداد خطة التشغيل الأولية

الشرح

١. وضع خطة تحديد المهام الأولى للمصدر وفق مستوى معلوماته وقدرته على التعاون.

٢. تحديد نقاط اللقاء الآمنة لتقليل التعرض.

٣. اختيار وسائل الاتصال المناسبة الهاتف المشفر، البريد الإلكتروني الآمن، أو اللقاءات المباشرة.

٤. وضع جدول زمني مرن للتواصل بما يتناسب مع جدول المصدر وبيئته.

المفهوم

١. التخطيط الجيد في البداية يقلل المخاطر التشغيلية ويضمن بدء العلاقة بشكل آمن ومنظم.

سيناريو عملي:

١. ضابط يعمل مع مصدر جديد داخل مؤسسة حكومية، يبدأ بطلب معلومات عامة عن العمليات اليومية قبل الانتقال لمعلومات حساسة، مع تحديد لقاء أسبوعي قصير وآمن

٢. بناء الحوافز

الشرح:

١. تحفيز المصدر من خلال مكافآت معنوية أو بسيطة شكر مباشر، تعزيز الثقة، تقديم معلومات مفيدة للمصدر.

٢. مراقبة توازن الحوافز لتجنب الإفراط أو سوء التقدير.

٣. ربط الحوافز بأداء المصدر وجودة المعلومات المقدمة.

المفهوم:

١. الحوافز المناسبة تعزز استمرارية التعاون وتزيد من جودة المعلومات.

سيناريو عملي

١. مصدر يقدم معلومات دقيقة حول مشروع حساس، يتم تقديم تقدير رسمي (شهادة، إشادة) ويُشجّع على الاستمرار بالمشاركة دون منح مكافآت مادية كبيرة قد تسبب ضغطًا لاحقًا.

٣. التقييم الدوري

الشرح

١. إجراء تقييم منتظم لجودة المعلومات ودقة التقرير.

٢. متابعة التزام المصدر بالبروتوكولات والسرية.

٣. استخدام مؤشرات الأداء عدد المعلومات الدقيقة، سرعة الرد، موثوقية البيانات.

المفهوم:

١. التقييم الدوري يتيح تحديد نقاط الضعف مبكرًا واتخاذ إجراءات تصحيحية، ويعزز إدارة المخاطر التشغيلية.

سيناريو عملي:

١. كل أسبوع، يتم جمع التقارير من المصدر ومراجعتها، ثم مناقشة نتائج التقييم معه بطريقة بنّاءة، مع تحديد خطوات تحسين إذا لزم الأمر.

٤. إدارة المخاطر الأولية للمصادر

الشرح:

١. تحديد التهديدات المحتملة: مراقبة، ضغط نفسي، تعرض لمعلومات حساسة غير آمنة.

٢. وضع خطط بديلة بسيطة في حال حدوث أي تهديد.

٣. تعريف المصدر بالإجراءات الأمنية الأولية للحفاظ على سلامته.

المفهوم:

١. إدارة المخاطر المبكرة تضمن استمرار العملية بشكل آمن وتحمي المصدر والضابط.

سيناريو عملي:

١. مصدر يعمل في مؤسسة حساسة، يتم تزويده بخطة بسيطة للتواصل في حال اكتشاف أي مراقبة، مثل تغيير مكان اللقاء أو استخدام قناة اتصال بديلة

٥. أدوات وتقنيات التشغيل الأساسية

١. قوالب خطة التشغيل الأولية: تشمل المهام، وسائل الاتصال، جدول المواعيد، نقاط الخطر المحتملة.

٢. سجل الحوافز والمتابعة: لتوثيق المكافآت والاعترافات وتحليل أثرها.

٣. قائمة مؤشرات الأداء KPI لتقييم جودة التقارير وسرعة الاستجابة والالتزام.

٤. لوائح الأمن الأولي تعليمات للمصدر حول حماية نفسه والمعلومات.

٦. التمارين العملية

١. محاكاة خطة تشغيل أولية: إنشاء خطة كاملة لمصدر افتراضي جديد مع تحديد المهام ونقاط الاتصال.

٢. تمرين متابعة الحوافز: تصميم حزمة تحفيزية لمصدر، وتقييم أثر كل بند على جودة المعلومات.

٣. ورشة تقييم دوري: مراجعة تقارير أسبوعية لمصدر افتراضي، واستخراج نقاط القوة والضعف ووضع توصيات.

٤. تمرين إدارة المخاطر إعداد سيناريو تهديد بسيط وكيفية التعامل معه بشكل آمن.

٧. المخرجات المتوقعة

١. القدرة على إعداد خطة تشغيل أولية آمنة وفعّالة.

٢. تصميم حزمة حوافز متوازنة تعزز الأداء وتقلل المخاطر.

٣. تنفيذ تقييم دوري لمصداقية وجودة المعلومات.

٤. وضع إجراءات أمنية أولية للمصدر تقلل احتمال التعرض للمخاطر.

الفصل التاسع

الدورات التشغيلية المتقدمة

١. تشغيل المصادر في بيئات معقدة

الشرح

١. إدارة وتشغيل المصادر ضمن مؤسسات حساسة أو جماعات معادية تتطلب مستوى عالي من التنظيم والمراقبة.

٢. تقييم المخاطر البيئية، القانونية، والثقافية قبل توجيه المهام.

٣. تطبيق بروتوكولات الأمان التشغيلي لحماية المصدر والضابط.

المفهوم

١. التعامل مع بيئات معقدة يزيد من احتمالية الأخطاء، لذا التخطيط المسبق ضروري لتقليل المخاطر وضمان استمرارية جمع المعلومات.

سيناريو عملي

١. مصدر يعمل داخل إدارة حكومية حساسة. الضابط يضع خطة تشغيل تشمل: لقاءات قصيرة محددة مسبقًا، استخدام وسيلة اتصال آمنة، مراجعة المعلومات مع الضابط قبل نشرها، وتقييم كل خطوة لضمان الأمان.

٢. إدارة اللقاءات منخفضة الرؤية

الشرح

١. تنظيم لقاءات آمنة وغير متوقعة لتقليل احتمالية التعرض للمراقبة.

٢. استخدام قنوات اتصال مخفية أو متغيرة.

٣. تحديد ساعات ومواقع اللقاء بعناية مع إعداد خطط بديلة للطوارئ.

المفهوم

١. اللقاءات منخفضة الرؤية تقلل من تعرض المصدر أو الضابط لأي تهديد أو كشف محتمل.

سيناريو عملي

١. لقاء مع مصدر حساس في منطقة عامة، مع تحديد نقاط دخول وخروج بديلة، واعتماد إشارات محددة مسبقًا لتنبيه الضابط بالمخاطر أو الحاجة لتأجيل اللقاء.

٣. هندسة العلاقة مع المصدر

الشرح

١. بناء علاقة ثقة طويلة الأمد تعتمد على الصراحة، السرية، والاحترام المتبادل.

٢. إدارة الحوافز بشكل مستمر ومتابعة الانفعالات والتحفيز للمصدر.

٣. إعادة ضبط العلاقة في حال حدوث فتور أو انقطاع .

المفهوم

١. العلاقة الجيدة تزيد من استمرارية التعاون وتحسن جودة المعلومات على المدى الطويل.

سيناريو عملي

١. مصدر بدأ يظهر تراجعًا في التعاون، الضابط يقوم بتقييم الأسباب: ضغط عمل، فقدان ثقة، أو ضعف تحفيز. يتم تعديل الحوافز وتوضيح خط سير العمل، ثم إعادة لقاء تدريجي لبناء الثقة.

٤. إدارة مهام متعددة في بيئات معقدة

الشرح

١. تنسيق مهام مختلفة مع مراعاة أولوية الأهمية والأمان.

٢. استخدام جداول تشغيل دقيقة مع تحديد المسؤوليات ومراقبة الأداء.

٣. دمج مهام المصدر مع شبكة معلوماتية واسعة لتقليل التعرض الفردي للمخاطر.

المفهوم

١. إدارة المهام المتعددة بطريقة منظمة تحافظ على سير العمل وتقلل المخاطر التشغيلية على المصادر والضباط.

سيناريو عملي

١. ضابط يدير ثلاثة مصادر في بيئات حساسة، يقوم بتوزيع المهام وفق أولوية جمع المعلومات، ويضع نقاط تحقق أسبوعية لضمان جودة المعلومات ومراعاة أمان كل مصدر.

٥. التقييم والتحليل التشغيلي

الشرح

١. إجراء تقييم مستمر للأداء من خلال متابعة تقارير المصادر ومؤشرات جودة المعلومات.

٢. تحليل المخاطر المرتبطة بكل مصدر وبيئة تشغيله.

٣. تطبيق أدوات قياس معيارية لتحديد نقاط القوة والضعف وتوجيه المصادر لتحسين الأداء.

المفهوم

١. التقييم والتحليل المستمر يضمن جودة المعلومات ويقلل المخاطر التشغيلية، ويساعد في اتخاذ قرارات سريعة وصحيحة.

سيناريو عملي

١. بعد أسبوع من العمل مع مصدر في بيئة معقدة، يتم جمع تقاريره وتحليل مؤشرات الأداء (دقة، سرعة، موثوقية) لتحديد ما إذا كان بحاجة لدعم إضافي، تعديل الحوافز، أو إعادة توجيه المهام.

٦. أدوات وتقنيات التشغيل المتقدمة

١. قوائم تحقق منخفضة الرؤية: لتحديد نقاط اللقاء والمخاطر المحتملة.

٢. سجلات متابعة الأداء: لتقييم المصادر بشكل دوري مع مؤشرات KPI محددة.

٣. قوالب إدارة الحوافز والعلاقة: لضمان استمرار التعاون وتحسين الأداء.

٤. لوائح الأمان التشغيلي: لإرشاد الضباط والمصادر في كل بيئة معقدة.

٧. التمارين العملية

١. محاكاة تشغيل مصدر في بيئة معقدة: إعداد خطة تشغيل كاملة مع نقاط لقاء آمنة ومؤشرات أداء محددة.

٢. تمرين إدارة اللقاءات منخفضة الرؤية: إنشاء سيناريو لقاء حساس وتحديد خطط بديلة للطوارئ.

٣. ورشة إعادة بناء العلاقة: حالة مصدر بدأ يظهر تراجعًا، وضع خطة لتحفيزه واستعادة الثقة.

٤. تقييم مهام متعددة: توزيع عدة مهام على مصادر مختلفة ومتابعة الأداء وتحليل المخاطر.

٨. المخرجات المتوقعة

١. القدرة على تشغيل مصادر في بيئات معقدة بأمان وفعالية.

٢. تصميم لقاءات منخفضة الرؤية وتقليل احتمالية كشف الهوية.

٣. إدارة العلاقة مع المصدر بشكل مستمر وتحسين جودة المعلومات.

٤. القدرة على توزيع المهام وتحليل الأداء لضمان جمع معلومات دقيقة وموثوقة.

تمام، إليك الفصل العاشر: تشغيل المصادر عالية الحساسية مفصّلًا بالكامل مع الشرح والمفاهيم والسيناريوهات العملية.

الفصل العاشر

تشغيل المصادر عالية الحساسية

١. مصادر داخل المؤسسات الحكومية

الشرح

١. التعامل مع موظفين لـديهم وصـول لمعلومـات حساسـة داخل المؤسسات الحكومية يتطلب دقة وحذر شديد.

٢. تقييم درجة النفوذ والوصول للمصدر قبل أي توجيه مهام.

٣. إنشاء خط اتصال آمن وموثوق لتبادل المعلومات.

المفهوم

١. حماية المصدر أثناء العمليات ضرورة قصوى، وأي تسرب قد يؤدي إلى كشف العملية أو المساس بأمن الدولة.

سيناريو عملي

١. ضابط يدير مصدر داخل وزارة الطاقة لديه وصول لبيانـات

مشاريع حساسة. يتم تحديد نقاط لقـاء سـرية، اسـتخدام تشـفير رقمي للمراسلات، وتقديم مهام صغيرة أولية لاختبار الالتزام قبـل توسيع نطاق العمل.

٢. مصادر داخل الأجهزة الأمنية

الشرح:

تشغيل مصادر داخـل أجهـزة الأمـن أو الاسـتخبارات يمثـل أعلى مستويات الحساسية والخطر.

تطبيق بروتوكولات أمان مضاعفة مثل تغييرات مكان العمـل، استخدام هوية رقمية، وتوزيـع المعلومـات علـى مراحـل لتقليـل الخطر.

إجراء تقييم دوري للمخاطر قبل كل مهمة أو لقاء.

المفهوم:

١. العمل مع مصادر أمنية عالية الحساسـية يتطلـب مسـتوى عالي من التخطيط والمراقبة لمنع أي تسرب أو كشف.

سيناريو عملي:

١. مصدر داخل جهاز أمنـي يقـدم معلومـات عـن تحركـات جهات معادية. الضـابط يحـدد مواعيـد دقيقـة للقـاءات قصـيرة،

استخدام وسيلة اتصال مشفرة، وإعداد خطة طوارئ في حال تعرض المصدر لأي ضغط أو تحقيق داخلي.

٣. مصادر ضمن جماعات معادية

الشرح:

١. تشغيل مخترقين ضمن كيانات معادية يتطلب إعداد بروتوكولات حماية دقيقة وخطط طوارئ متعددة.

٢. مراقبة البيئة الاجتماعية والسياسية للجماعة لتجنب كشف المصدر.

٣. توفير دعم مستمر للمصدر، بما في ذلك إشارات آمنة للتواصل، وإجراءات الخروج الآمن عند الحاجة.

المفهوم:

١. تشغيل مصادر ضمن جماعات معادية يحمل أعلى المخاطر، لكن يوفر معلومات نوعية يمكن أن تكون حاسمة للعمليات الاستخباراتية.

سيناريو عملي

١. مصدر يعمل داخل جماعة معادية. الضابط يحدد أسلوب اتصال مشفر عبر الإنترنت، نقاط لقاء آمنة ضمن بيئة عامة، وخطة

طوارئ تتضمن غطاء وظيفي للمصدر وإرشادات محددة للتعامل مع أي مراقبة.

٤. إدارة المخاطر والاحتياطيات

الشرح

وضع خطط احتياطية متعددة لكل مصدر عالي الحساسية، تشمل:

١. نقاط خروج آمنة.

٢. وسائل اتصال بديلة.

٣. بروتوكولات لتقييم الوضع في حالات الطوارئ.

٤. تقييم مستمر لمستوى الخطر وتأثيره على الضابط والمصدر.

المفهوم

١. إدارة المخاطر بشكل استباقي تضمن استمرار العملية وتقليل فرص الفشل أو الضرر للمصادر.

سيناريو عملي:

١. عند حصول تهديد مفاجئ للمصدر، يتم تفعيل خطة الطوارئ: إخراج المصدر من الموقع، تغيير وسيلة الاتصال، وإبلاغ الضابط بمرحلة آمنة قبل استئناف العمليات.

٥. أدوات وتقنيات التشغيل عالية الحساسية

١. لوائح حماية المصدر إجراءات محددة لضمان سرية الهوية.

٢. تشفير رقمي متقدم حماية الاتصال الرقمي والمراسلات السرية.

٣. خطة طوارئ متعددة الطبقات إعداد بدائل للطوارئ، بما في ذلك تغطية قانونية واجتماعية.

٤. تقييم مستمر للمخا طر تحليل التهديدات والتغيرات في البيئة التشغيلية.

٦. التمارين العملية

١. تمرين تشغيل مصدر داخل جهاز أمني وضع خطة تشغيل، خطوط اتصال آمنة، ومتابعة الأداء مع تقييم المخاطر.

٢. محاكاة تشغيل مصدر ضمن جماعة معادية إنشاء غطاء وظيفي واجتماعي، اختبار الاتصال، وتطبيق خطط الطوارئ.

٣. ورشة إدارة الطوارئ: اختبار سيناريوهات تهديد مفاجئ للمصدر وكيفية التعامل الفوري.

٤. تقييم الأداء عالي الحساسية: تحليل جودة المعلومات، مستوى أمان المصدر، وتقديم توصيات لتحسين العمل المستقبلي.

٧. المخرجات المتوقعة

١. القدرة على تشغيل مصادر عالية الحساسية بأمان وفعالية.

٢. تصميم وتنفيذ خطط طوارئ متعددة الطبقات.

٣. إدارة المخاطر بشكل استباقي وضمان استمرار جمع المعلومات.

٤. تحسين جودة المعلومات من مصادر حساسة، مع الحفاظ على أمن الضابط والمصدر.

الفصل الحادي عشر

الأمن الرقمي و Cyber-HUMINT تطويري

١. تجنيد وتشغيل المصادر عبر الإنترنت

الشرح

١. بناء هوية رقمية كاملة (Digital Legend) للمصدر لضمان مصداقيته وسرية هويته.

٢. فتح خطوط تشغيل آمنة داخل بيئات رقمية مغلقة مثل المنتديات السرية، الشبكات المغلقة، أو التطبيقات المشفرة.

٣ تقييم مستوى التفاعل الرقمي للمصدر، ومدى قدرته على تقديم المعلومات عبر الإنترنت دون كشف هويته.

المفهوم

Cyber-HUMINT يعتمد على الجمع بين المهارات البشرية التقليدية وأساليب العمل الرقمي لحماية الهوية وتحقيق أفضل النتائج.

سيناريو عملي

١. ضابط يشرف على مصدر يعمـل ضـمن مجموعـة مغلقـة علـى الإنترنـت. يقـوم بإنشـاء هويـة رقميـة متكاملـة، ويحـدد بروتوكولات اتصال مشفرة، ثم يوجّـه المصـدر لجمـع معلومـات دقيقة عن أهداف محددة دون التعرض لأي كشف.

٢. تأمين الأجهزة الرقمية

الشرح

١. استخدام أجهزة آمنة ومشفرة للاتصال مع المصادر.

٢.تطبيق تقنيات التشفير الحديث ومراقبة جميع المحاولات غير المصرح بها للوصول إلى البيانات.

٣. إعداد خطط نسخ احتياطي آمن لتفادي فقدان البيانات في حال اختراق الأجهزة.

المفهوم

١. حماية الأجهزة الرقمية جزء أساسـي مـن الأمـن الرقمـي، حيث أن أي تسرب قد يؤدي لكشف المصدر أو العمليات.

سيناريو عملي

١. مصدر يعمل مـن جهـاز شخصـي فـي بيئـة غيـر مأمونـة.

الضابط يوفّر له جهازًا آمنًا، يثبت عليه برامج تشفير، ويضع تعليمات دقيقة لتحديث الجهاز دورياً وتجنب أي روابط مشبوهة.

٣. التعامل مع التهديدات السيبرانية

الشرح

١. اكتشاف محاولات الاختراق المبكرة وتحليل مصادرها.

٢. تصنيف التهديدات حسب خطورتها واتخاذ الإجراءات اللازمة.

٣. حماية هوية المصدر من أي كشف أو اختراق قد يؤثر على العملية.

المفهوم

١. التهديدات السيبرانية يمكن أن تكون أكثر خطورة من التهديدات الميدانية، لأنها قد تكشف جميع عناصر العملية دفعة واحدة.

سيناريو عملي

١. اكتشاف محاولة اختراق لخط الاتصال الرقمي للمصدر. يتم إيقاف الاتصال فوراً، تغيير قنوات الاتصال، وتحليل المخاطر لتحديد مصدر التهديد، مع تفعيل خطة طوارئ لحماية المصدر.

٤. إدارة الهوية الرقمية للمصدر

الشرح:

١. تطوير ملف رقمي كامل للمصدر يشمل اسمًا مستعارًا، تاريخًا رقميًا، وسلوكًا افتراضيًا متوافقًا مع البيئة التشغيلية.

٢. تحديث الهوية الرقمية باستمرار لضمان الاستدامة التشغيلية ومنع أي كشف محتمل.

المفهوم

١. الهوية الرقمية آمنة تعني قدرة أكبر على تشغيل المصادر دون تعريضهم أو العملية للخطر.

سيناريو عملي

١. إنشاء هوية رقمية لمصدر داخل منتدى مغلق. يتم تحديث النشاط الرقمي، محاكاة سلوك طبيعي، ومراقبة أي استفسارات قد تكشف الهوية الحقيقية للمصدر.

٥. بروتوكولات الاتصال الآمن

الشرح

١. تحديد طرق اتصال متعددة ومشفرة بين الضابط والمصدر.

٢. إنشاء قنوات احتياطية في حال اختراق القناة الرئيسية.

٣. تدريب المصدر على الاستخدام الصحيح للقنوات المشفرة، وعدم استخدام أي وسائل غير موثوقة.

المفهوم

١. حماية الاتصال الرقمي أمر حاسم لاستمرارية العمليات وتجنب كشف المصدر.

سيناريو عملي

١. مصدر يرسل معلومات عبر برنامج مشفر. يتم وضع قناة اتصال ثانية بديلة، والتأكد من أن الرسائل لا تحتوي على أي بيانات تكشف المصدر أو العملية.

٦. تحليل المخاطر الرقمية

الشرح

١. تقييم مستوى تهديدات الإنترنت، البرامج الخبيثة، والجهات المعادية.

٢. تحليل السلوك الرقمي للمصدر لتحديد أي مؤشرات على اختراق أو ضعف الأمان.

٣. إعداد خطط وقائية تشمل تحديثات أمنية، إزالة ثغرات، ومراقبة مستمرة.

المفهوم

١. التحليل المستمر يقلل من فرص الفشل الرقمي ويحمي هوية ومعلومات المصدر.

سيناريو عملي

١. تحليل الشبكة التي يعمل فيها المصدر، كشف ثغرة في تطبيق التواصل، تنفيذ تحديث أمني سريع، وتحذير المصدر من أي تصفح مشبوه قد يعرض العملية للخطر.

٧. تمارين عملية

١. تمرين إنشاء هوية رقمية متكاملة تطوير Digital Legend شامل للمصدر.

٢. تمرين الاتصال الآمن استخدام قنوات مشفرة متعددة مع بروتوكولات طوارئ.

٣. محاكاة اختراق التعامل مع تهديد سيبراني مفاجئ وتحليل المخاطر لحماية المصدر.

٤. ورشة تحليل السلوك الرقمي للمصدر قراءة الأنماط الافتراضية للمصدر، تحديد أي علامات على اختراق أو كشف الهوية.

٨. المخرجات المتوقعة

١. القدرة على تجنيد وتشغيل مصادر عبر الإنترنت بأمان وفعالية.

٢. حماية الهوية الرقمية للمصدر ومنع أي كشف محتمل.

٣. إدارة المخاطر السيبرانية بفعالية عالية.

٤. توظيف Cyber-HUMINT لدعم العمليات الاستخباراتية في البيئات الرقمية المغلقة والمعقدة.

الفصل الثاني عشر

التحليل البيومتري والسلوكي المتقدم

١. التحليل الصوتي والسلوكي

الشرح

١. مراقبة تغييرات نبرة الصوت، سرعة الكلام، مؤشرات التوتر الدقيقة أثناء المقابلات أو الاتصالات.

٢. تحليل الحركة والجسد مثل تحريك اليدين، الميل نحو الخلف أو الأمام، ومؤشرات العين.

٣. استخدام أدوات تسجيل وتحليل صوتي متقدمة لتحديد الصدق أو الخداع.

المفهوم

١. قراءة المؤشرات البيومترية والسلوكية تساعد الضابط على فهم الحالة النفسية للمصدر، مدى صدقه، واستعداده للتعاون.

سيناريو عملي :

١. خلال مقابلة مع مصدر محتمل، يلاحظ الضابط زيادة سرعة الكلام عند سؤال حساس. يتم استخدام جهاز تسجيل صوتي لتحليل الترددات الصوتية ومؤشرات التوتر، لتقييم مدى صدق المصدر قبل إعطاء مهام حساسة.

٢. الخرائط السلوكية للمصدر

الشرح

١. إنشاء ملفات سلوكية دقيقة لكل مصدر، تشمل أنماط الاستجابة، نقاط القوة، ومواطن الضعف.

٢. متابعة السلوك اليومي للمصدر ومقارنة التغيرات مع المعايير السابقة.

٣. استخدام هذه الخرائط لتوقع ردود الفعل وتحسين التوجيهات التشغيلية.

المفهوم

١. كل مصدر له نمط سلوكي فريد وفهم هذا النمط يزيد من فعالية إدارة المهام وحماية العملية.

سيناريو عملي

١. مصدر يعمل ضمن بيئة حساسة، يقوم الضابط برصد سلوكياته اليومية عبر لقاءات قصيرة أو مراقبة غير مباشرة. يتم تسجيل المؤشرات في ملف رقمي، ومقارنتها بالبيانات السابقة لتوقع ردود فعل المصدر عند تقديم مهمة حساسة.

٣. كشف الخداع المتقدم

الشرح

١. التعرف على المؤشرات الدقيقة للانحراف عن الصدق مثل التباطؤ في الإجابة، التناقض في المعلومات، وتغيرات الميكروفيسيولوجية.

٢. تحليل الاستجابة تحت الضغط العالي مثل أسئلة مفاجئة أو سيناريوهات اختبارية.

٣. توظيف تقنيات المراقبة البيومترية الحديثة للكشف عن أي محاولة خداع.

المفهوم

القدرة على كشف الخداع بشكل متقدم توفر حماية أكبر للعمليات وتحمي الضابط من الاعتماد على معلومات مضللة.

سيناريو عملي

١. اختبار مصدر يعمل داخل جماعة معادية. يتم طرح أسئلة دقيقة ومفاجئة، مراقبة التغيرات الصوتية والحركية، وتحليل النتائج لتحديد ما إذا كان المصدر صادقًا أم يحاول إخفاء معلومات.

٤. دمج التحليل البيومتري معCyber-HUMINT

الشرح

١. استخدام البيانات السلوكية والبيومترية مع البيانات الرقمية لتقييم مصداقية المعلومات التي يقدمها المصدر عبر الإنترنت.

٢. مراقبة سلوك المصدر الرقمي مثل سرعة الرد، أسلوب الكتابة، ونمط التفاعل، وربطه بالملفات البيومترية السابقة.

المفهوم

١. الدمج بين HUMINT التقليدي والتحليل الرقمي يزيد من دقة التقييم وتقليل المخاطر.

سيناريو عملي

١. مصدر يرسل تقارير رقمية عن نشاط جماعة معادية. يتم مقارنة سرعة الكتابة وتغير النبرة الرقمية مع الخرائط السلوكية

لسابقة، للتأكد من التوافق مع سلوكه الطبيعي وكشف أي مؤشرات خديعة أو ضغط.

٥. أدوات وتقنيات التحليل البيومتري

الشرح

١. برامج تحليل الصوت والنبرة لتحديد الصدق والتوتر.

٢. أجهزة تتبع الحركة وحركات العين في المقابلات الحية.

٣. أنظمة إدارة الخرائط السلوكية الرقمية لتسجيل ومتابعة تطور السلوك على المدى الطويل.

المفهوم

١. الأدوات البيومترية تزيد من موضوعية التقييم وتحمي العملية من الانحرافات البشرية في الحكم.

سيناريو عملي

١. مقابلة مع مصدر داخلي حساس، استخدام كاميرات ومجسات غير مباشرة لرصد مؤشرات التوتر، وتحليل النتائج لمطابقتها مع تقارير سابقة لتحديد موثوقية المعلومات المقدمة.

٦. تمارين عملية

١. تمرين تحليل الصوت والنبرة: تسجيل مقابلات قصيرة

للمصادر، وتحليل الترددات ونقاط التوتر.

٢. تمرين الخرائط السلوكية: إنشاء ملف سلوكي رقمي لمصدر ومتابعة التغيرات اليومية.

٣. تمرين كشف الخداع إعداد سيناريو أسئلة مفاجئة وتحليل الاستجابة البيومترية والسلوكية.

٤. ورشة الدمج الرقمي والبيومتري: مقارنة السلوك الرقمي للمصدر مع البيانات البيومترية للتحقق من التوافق ومصداقية المعلومات.

٧. المخرجات المتوقعة

١. القدرة على تقييم دقيق للمصدر بناءً على التحليل البيومتري والسلوكي.

٢. كشف الخداع بشكل متقدم وتقليل المخاطر التشغيلية.

٣. توظيف التحليل البيومتري لدعم القرارات التشغيلية في البيئات الحساسة والمعقدة.

٤. دمج HUMINT التقليدي و Cyber-HUMINT لتحقيق أقصى فعالية في إدارة وتشغيل المصادر.

الفصل الثالث عشر

التكتيكات المتقدمة والمراقبة المضادة

١. المراقبة الميدانية المتقدمة

الشرح

١. تتضمن تتبع الهدف والمصادر دون الكشف عن هوية الضابط أو العملية

٢. استخدام مركبات مزودة بأجهزة مراقبة، كاميرات خفية، وتقنيات GPS متقدمة

٣. تطبيق طرق التنقل والتواجد المنخفض الرؤية لتقليل احتمالية اكتشاف العملية من قبل جهات معادية

المفهوم

١. الحفاظ على سرية العملية وحماية المصدر والضابط عن طريق أساليب مراقبة ذكية ومخفية.

سيناريو عملي

١. مراقبة مصدر داخل مؤسسة حساسة، يتم استخدام سيارة مراقبة غير ملحوظة، كاميرات مخفية داخل المكان، وتقنيات تتبع ذكية لمتابعة تحركات المصدر بدون لفت الانتباه.

٢. كشف المراقبة

الشرح

١. تطبيق تقنيات تحديد وجود مراقبين أو تهديدات محتملة خلال التنقل أو اللقاءات.

٢. مراقبة البيئة المحيطة، مثل الأشخاص الغريبين، المركبات المتكررة، أو استخدام أجهزة الكشف عن أجهزة التنصت.

٣. اعتماد بروتوكولات تحليل المخاطر اللحظية واتخاذ إجراءات مضادة فورية

المفهوم

القدرة على اكتشاف أي تهديد محتمل قبل أن يؤثر على سلامة العملية أو المصدر.

سيناريو عملي

أثناء خروج المصدر من المؤسسة، يلاحظ الضابط مركبة

تتبع حركته، يستخدم تقنيات تغيير المسار والاختفاء المؤقت، لتجنب أي مراقبة محتملة دون فقدان الهدف.

٣. التخفي وتغيير الهوية

الشرح

١. بناء غطاء وظيفي واجتماعي كامل للضابط أو المصدر عند الحاجة.

٢. إدارة الوثائق الداعمة، الوسائل التقنية، وأسلوب السلوك بما يتوافق مع الهوية المزيفة.

٣. وضع استراتيجية هروب وخروج آمن في حال تعرض العملية للخطر.

المفهوم

١. التخفي المتقن يحمي العملية والمصدر ويتيح تنفيذ المهام في بيئات معادية.

سيناريو عملي

١. ضابط يعمل ضمن جماعة معادية يحتاج للقاء مصدر، يتم تهيئة هوية مزيفة تشمل بطاقة تعريف، مظهر وظيفي، وسلوكيات يومية متناسقة مع الغطاء، مع خطة خروج احتياطية في حال الشك أو الكشف.

٤. المراقبة المضادة

الشرح

١. إجـراءات كشـف ومحاصـرة أي محـاولات للمراقبـة أو التعقب من قبل أجهزة معادية.

٢. استخدام تقنيات الانحـراف، التمويـه، والالتفـاف الـذكي لإرباك أي طرف يراقب العملية.

٣. تنفيـذ اختبـارات منتظمـة علـى طـرق الحركـة والأمـاكن المستخدمة لضمان أمان العمليات.

المفهوم

١. مراقبة مضادة فعالة تقلـل مـن فـرص تعـرض المصـدر أو الضابط لأي تهديد وتشير إلى أي اختراق محتمل للسرية.

سيناريو عملي

أثناء نقل معلومات حساسة، يـتم تطبيـق مسـار مـزدوج، مـع استخدام مركبات بديلة وأجهزة اتصال مشفرة لتجنب أي محاولـة تنصت أو تتبع من جهات معادية.

٥. دمج التكتيكات مع HUMINT وCyber-HUMINT

الشرح

١. مراقبة ميدانية متقدمة تتكامل مع تحليل السلوك الرقمي للمصدر

٢. متابعة الأنشطة الرقمية للمصدر على شبكات مغلقة، وربطها بالمراقبة الميدانية للتحقق من الالتزام بالأدوار والبروتوكولات.

المفهوم

الدمج بين المراقبة الميدانية والتحليل الرقمي يزيد من دقة المتابعة ويحمي العمليات من الانكشاف.

سيناريو عملي

مصدر يعمل ضمن جماعة معادية، يتم متابعة تحركاته ميدانيًا مع رصد تفاعلاته الرقمية، ومطابقة السلوكين لضمان مصداقية المعلومات وسلامة العملية.

٦. تمارين عملية

١. تمرين المراقبة المنخفضة الرؤية تدريب الضباط على تتبع الهدف دون لفت الانتباه باستخدام مركبات وأجهزة مخفية.

٢. تمرين كشف المراقبة إعداد سيناريوهات لاختبار قدرة الضباط على اكتشاف مراقبين أو أجهزة تنصت محتملة.

٣. ورشة التخفي وتغيير الهوية إنشاء هوية مزيفة كاملة للمصدر أو الضابط وتجريب لقاءات عملية آمنة.

٤. تمرين المراقبة المضادة تنفيذ اختبار شامل لمسارات وآليات الحركة لضمان أمان العملية وسلامة المصدر

٧. المخرجات المتوقعة

١. القدرة على تنفيذ عمليات HUMINT في بيئات معادية بأمان وفعالية.

٢. تطوير مهارات المراقبة المتقدمة وكشف المراقبة

٣. حماية المصادر والضباط عبر التخفي، التمويه، وتغيير الهوية عند الحاجة.

٤. تكامل المراقبة الميدانية مع Cyber-HUMINT لتعزيز دقة التقييم والأمان العملياتي.

الفصل الرابع عشر

بناء شبكات المصادر متعددة الطبقات

(Multi-Layered Source Networks Development)

شبكات المصادر متعددة الطبقات تُعدّ من أقوى الهياكل الاستخباراتية التي تضمن الوصول المستمر للمعلومات من عدة مستويات داخل البيئة الهدف، وتمنح الضابط القدرة على قراءة الواقع من نقاط مختلفة دون كشف الشبكة أو المصدر الأساسي.

أولًا: مفهوم الشبكات متعددة الطبقات

الشرح

تعتمد على توزيع المصادر على طبقات مختلفة بحسب مستوى وصولهم، أدوارهم، ودرجة حساسيتهم.

الهدف هو خلق بنية هرمية أو حلقية قادرة على توفير معلومات متقاطعة (Cross-Validation) لضمان صحة البيانات ومنع التضليل.

توفر بدائل في حال سقط أو انكشف أحد المصادر.

المفهوم

شبكة متينة تتكون من مصادر في الدائرة الخارجية، الوسطى، والداخلية، كل منهم له دور محدد ومعلومات مختلفة تُكمل بعضها.

ثانيًا: أنواع الطبقات في الشبكات الاستخباراتية

١. الطبقة الخارجية(Outer Layer)

الشرح

١. تشمل مصادر ذات وصول محدود للمعلومة الحساسة.

٢.توفر مؤشرات عامة ودلالات أولية على البيئة المستهدفة.

٣.غالبًا ما تكون مصادر منخفضة الخطر ويمكن تعويضها بسهولة.

أمثلة

١. سائقي النقل، عمال الخدمات، موظفين ذوي صلة غير مباشرة.

سيناريو

مصدر خارجي يعمل في شركة خدمات أمنية يقدم مؤشرات عن مستوى الحراسة قبل محاولة اختراق أو دخول مرتبط بالمعلومات.

٢. الطبقة الوسطى(Middle Layer)

الشرح

١. مصادر لها وصول متوسط، يـزوّدون الضـابط بمعلومـات تحليليّة أعمق.

٢. دعم عملية التحقق المتقاطع مع الطبقة الداخلية.

٣. غالبًا يكونون على دراية بآليات العمل اليومية في المؤسسة.

أمثلة

موظفين إداريين، فنيين، مشرفين، شركاء عمل.

سيناريو

فني في شبكة تقنية يوفر بيانات عن تحديثات أنظمة الحماية، مما يساعد على رسم صورة أدق للبيئة التقنية للهدف.

٣. الطبقة الداخلية (Inner Layer)

الشرح

١. مصادر حساسـة للغايـة ذات وصـول مباشـر للمعلومـات السرية أو القرارات العليا.

٢. يمثلون عصب الشبكة ويجب إدارتهم بعناية فائقة.

٣. يستلزم تشغيلهم وجود خطـط حمايـة مضـاعفة وضـوابط

سرية عالية.

أمثلة

ضباط، إداريون كبار، خبراء تقنيون مرتبطون مباشرة بعمليات حساسة، أو أعضاء في شبكة داخلية للخصم.

سيناريو

مصدر داخلي في مركز اتخاذ القرار يرسل إحداثيات أو خطط عمليات سيتم تنفيذها خلال ٤٨ ساعة، مما يسمح بتفعيل تدابير دفاعية أو هجوم مضاد.

ثالثًا: منهجيات بناء الشبكة متعددة الطبقات

١. التدرج في التجنيد

الشرح

يبدأ الضابط بتجنيد مصادر من الطبقة الخارجية ثم الوسطى، ثم يصل تدريجيًا للطبقة الداخلية.

هذا التدرج يمنح الضابط فهمًا عميقًا للبيئة ويقلّل من المخاطر.

نقطة قوة

يتم اكتشاف الثغرات واحتياجات المعلومات قبل الوصول للمصادر الأكثر حساسية.

٢. بناء شبكة الاحتياط (Backup Layer)

الشرح

١. مجموعة مصادر احتياطية تُستخدم عند سقوط أحد المصادر.

٢.ئتوفر استمرارية للمعلومات وتمنع الانقطاع العملياتي.

سيناريو

تم كشف مصدر داخلي، فيتم تفعيل مصدر احتياطي لديه وصول من الطبقة الوسطى لتقليل أثر الخسارة.

٣. الربط غير المباشر بين الطبقات

الشرح

١. يمنع التواصل أو المعرفة بين المصادر.

٢. كل مصدر يعتقد أنه المصدر الوحيد.

٣. يقلّل فرص كشف الشبكة في حال اختراق طبقة واحدة.

حالة تطبيقية

مصدر داخلي لا يعرف بوجود مصادر خارجية أو وسطى، وبالتالي لا يستطيع كشف الشبكة بالكامل.

رابعًا: إدارة الشبكة متعددة الطبقات

١. مبدأ "العزل الطبقي"

الشرح

عزل كل طبقة بمهام مستقلة، رغم أن جميعها تخدم الهدف نفسه.

الفائدة

يمنع كشف الشبكة حتى في حال انهيار جزء منها.

٢. التحليل المتقاطع للمعلومات

الشرح

١. مقارنة المعلومات بين مصادر من طبقات مختلفة.

٢. اكتشاف التضليل أو الأخطاء.

سيناريو

المصدر الداخلي يبلغ عن تغييرات أمنية، بينما المصدر الخارجي يبلغ عن زيادة في الدوريات، فيتم تأكيد المعلومات.

٣. إدارة المخاطر لكل طبقة

الشرح

١. الطبقة الداخلية تُعدّ الأعلى خطرًا وتتطلب مراقبة أكثر دقة.

٢. الطبقة الخارجية أقل خطورة لكنها تحتاج متابعة دائمة.

مؤشرات الخطر

١. تغيّر سلوك المصدر.

٢. معلومات متناقضة.

٣. رسائل ضغط من البيئة المعادية.

خامسًا: بناء الثقة بين المصادر والقائم بالتشغيل

١. تعزيز الدافعية لكل طبقة

١. الخارجية: مكافآت بسيطة - دعم وظيفي - تسهيلات.

٢. الوسطى: دعم مالي - توفير أدوات - حماية.

٣. الداخلية: حماية سرية - ضمانات - خطط خروج - دعم نفسي.

٢. آليات التواصل الآمن

١. بريد مشفر.

٢. لقاءات منخفضة الرؤية.

٣. قنوات مراسلة مشفرة عبر أجهزة غير متصلة.

٤. نقاط اتصال مُدارة (Dead Drops) .

سادسًا: سيناريوهات تشغيل احترافية

سيناريو ١: شبكة لاختراق مؤسسة أمنية

١. مصدر خارجي: سائق يعرف مداخل المبنى.

٢. مصدر وسط: فني شبكات يقدم مخطط الأنظمة.

٣. مصدر داخلي: ضابط غرفة العمليات.

٤. يتم دمج المعلومات لبناء صورة كاملة تُستخدم للتخطيط لعملية HUMINT حساسة.

سيناريو ٢: كشف تسريب داخلي في منظمة معادية

١. الخارجية: مراقبة الشحنات + موظف استقبال.

٢. الوسطى: موظف محاسبة يكتشف تغير التدفقات المالية.

٣. الداخلية: مصدر مُجند ضمن الدائرة الضيقة.

٤. التحليل المتقاطع يكشف الشخص المتهم بدقة.

سيناريو ٣: دعم عمليات دفاعية ضد تهديدات خارجية

شبكة على ثلاث طبقات تتنبأ بتحركات قوات معادية، عبر مصادر مختلفة المستويات، مما يسمح بقيادة عملية دفاعية ناجحة.

سابعًا: المخرجات المتوقعة

١. القدرة على بناء شبكة استخباراتية قوية ومتعددة المستويات.

٢. حماية الضابط والمصادر عبر طبقات عزل متقنة.

٣. ضمان ١٠٠٪ استمرارية المعلومات حتى في البيئات عالية التهديد.

٤. إنتاج تحليل استخباراتي دقيق وقابل للاستخدام الفوري في العمليات.

الفصل الخامس عشر

القيادة والإشراف العملياتي المتقدم

(Advanced Operational Leadership & Oversight)

يُعـدّ هـذا الفصـل مـن أخطـر وأهـم الفصـول فـي تشـغيل المصادر، لأنه ينتقل بالضابط من مستوى التشـغيل الفـردي إلـى مستوى القيادة والإدارة لعدة مصادر أو شـبكة كاملـة، مـع اتخـاذ قرارات معقدة ضمن بيئات عالية التهديد.

أولًا: مفهوم القيادة العملياتية فيHUMINT

الشرح

القيادة العملياتية تُعنى بقدرة الضابط على إدارة عدة مصـادر، تحليل المعلومات، توجيه الجهد الاستخباراتي، وحماية العمليـة من الانهيار أو التداخل.

المفهوم

القيادة ليست مجرد إصدار أوامر، بل:

١. قراءة الموقف.

٢. توقع المخاطر.

٣. اتخاذ قرارات دقيقة تحت الضغط.

٤. الحفاظ على السرية والتناغم بين الطبقات.

ثانيًا: إدارة الفرق متعددة المصادر (Multi-Source Management)

١. مبدأ فصل الأدوار (Role Segregation)

الشرح

يجب أن يُعطى كل مصدر مهامًا مستقلة لا تتقاطع بشكل يكشف الشبكة.

التطبيق

١. لا تطلب من مصدر خارجي ما يمكن أن يثير الشبهات.

٢. لا تسمح للمصدر الداخلي بمعرفة وجود مصادر أخرى.

٢. مبدأ الأوزان الاستخباراتية(Intelligence Weighting)

الشرح

بعض المصادر لها وزن أكبر لأن معلوماتهم أكثر حساسية أو دقة.

التقييم يتم عبر

١. طبيعة الوصول.

٢. جودة المعلومات.

٣. توقيت الحصول عليها.

مثال

معلومة من مصدر داخلي قد تساوي ١٠ معلومات من مصادر خارجية.

٣. تنظيم جدول التشغيل (Operational Calendar)

الشرح

يجب تحديد:

١. مواعيد اللقاءات.

٢. أوقات الاتصال.

٣. خطوط الطوارئ.

٤. نقاط التسليم (Dead Drops / Live Drops).

الفائدة

يمنع تضارب العمليات ويقلل المخاطر.

ثالثًا: اتخاذ القرارات تحت الضغط (Decision-Making Under Stress)

١. نموذج OODA في اتخاذ القرارات

OODA = Observe - Orient - Decide - Act

الشرح

يستخدم الضابط هذا النموذج أثناء المواقف الخطرة لتسريع القرار وضمان دقته.

المفهوم

Observe : مراقبة الوضع.

Orient : تحليل المعلومات.

Decide : اختيار القرار المناسب.

Act: التنفيذ الفوري مع خطة بديلة.

٢. إدارة العمليات في بيئات متغيرة

أمثلة على التغير المفاجئ

١. مراقبة على المصدر.

٢. استجواب داخلي في المؤسسة الهدف.

٣. تفتيش مفاجئ على الهواتف.

٤. تغيير عنوان العمل أو دور المصدر.

طريقة الإدارة

١. وضع سيناريوهات سابقة الإعداد.

٢. بناء خطوط خروج آمنة.

٣. تحديد رسائل إنذار تكتيكية (Trigger Words)

٣. القرار السريـع مقابل القرار العميق

الشرح

١. القرار السريع: للتعامل مع تهديد لحظي.

٢. القرار العميق: لتحريك المصدر نحو هدف بعيد.

المفهوم

الضابط المحترف يعرف متى يجـب أن يكـون سـريعًا ومتـى يجب أن يتأنّى.

رابعًا: تحليل المعلومات متعدد المصادر(Cross-Source Analysis)

١. قواعد الدمج والتحقق

الشرح

دمج المعلومات من:

١. مصادر بشرية.

٢. مصادر تقنية.

٣. مراقبة ميدانية.

٤. مصادر عبر الإنترنت.

الفائدة:

إزالة التضليل، وتحسين دقة التقييم العملياتي.

٢. كشف التضليل الداخلي

الشرح

قد يخدع المصدر الضابط لأسباب:

١. خوف.

٢. ضغط.

٣. مصلحة شخصية.

٤. إعادة توجيه من جهة معادية.

علامات التضليل

١. تناقضات زمنية.

٢. اختلاف اللهجة.

٣. مبالغات غير منطقية.

٤. محاولة توجيه الضابط لزاوية معينة.

٣. الخرائط التحليلية (Intelligence Mapping)

الشرح

إنشاء خريطة معلوماتية تربط:

١. الأشخاص.

٢. العلاقات.

٣. الأحداث.

٤. المواقع.

٥. التوقيتات.

الفائدة

تكشف الثغرات والمنـاطق المجهولـة التـي تحتـاج مصـدرًا إضافيًا.

خامسًا: ضبط التضارب بين المصادر(Conflict De-confliction)

١. أنواع التضارب

١. تضارب معلوماتي.(Conflicting Info)

٢. تضارب في الأدوار.

٣. تضارب في الحركة داخل نفس المؤسسة.

٤. تضارب يؤثر على السمعة العملياتية.

٢. طرق معالجة التضارب

١. التحقق المتقاطع.

٢. تعديل المهام.

٣. إعادة توزيع المصادر.

٤. إبطال أحد المصادر إذا ثبت تضليله.

٣. منع التضارب قبل حدوثه

الشرح

١. التخطيط الدقيق.

٢. تحديد مناطق نفوذ لكل مصدر.

٣. منع أي تواصل مباشر أو غير مباشر بينهم.

سادسًا: القيادة النفسية للمصادر(Psychological Leadership)

١. التفاف المصدر حول الضابط(Operator Gravity)

الشرح

١. حماية نفسية.

٢. ثقة عالية.

٣. شعور بالإنجاز.

الفائدة

المصدر يصبح أكثر التزامًا وأقل ميلًا للانحراف.

٢. بناء الولاء العملي وليس العاطفي

الشرح

ولاء المصدر يجب أن يكون:

١. للمصلحة.

٢. للأمان.

٣. للاستقرار.

وليس لشخص الضابط. (الضابط مرحلة قابلة للتغير)

٣. تصحيح انحراف السلوك

الشرح

إذا بدأ المصدر يتراخى أو يتهرب:

١ إعادة ضبط العلاقة.

٢ جلسة تقييم.

٣تحديد محفزات جديدة.

٤ تهدئة المخاوف.

سابعًا: سيناريوهات تطبيقية متقدمة

سيناريو ١: إدارة شبكة أثناء حالة طوارئ

١. سقوط مصدر داخلي.

٢.انقطاع الاتصال مع مصدر وسط.

٣. زيادة المراقبة الأمنية.

القيادة المطلوبة

تفعيل خط الطوارئ، استخدام مصدر خارجي لحماية الشبكة، وتصفير الاتصالات لمدة ٤٨ ساعة.

سيناريو ٢: تضارب معلوماتي عالي الخطورة

١. مصدر داخلي يقول إن هناك عملية قادمة.

٢. مصدر خارجي ينفي.

٣. مصدر إلكتروني يقدم إشارة متناقضة.

الحل

دمج وتحليلOODA ، وزيارة بقعة الميـدان، وتقيـيم تـاريخ كل مصدر.

سيناريو ٣: قيادة عملية تشغيل داخل مؤسسة معادية

١. ثلاث طبقات تعمل داخل بيئة معادية.

٢. خطر كشف داخلي مرتفع.

٣. ضرورة الحصول على معلومة خلال ٧٢ ساعة.

العمل

إعـادة توزيـع المهـام، إعطـاء مصـدر خـارجي دور الـدعم، وتفعيل أدواتCyber-HUMINT .

ثامنًا: مخرجات التعلم لهذا الفصل

١. القدرة على إدارة عدة مصادر ضمن شبكة واحدة.

٢. اتخاذ قرارات دقيقة في بيئات شديدة التهديد.

٣. تحليل المعلومات من عدة مصادر بشكل احترافي.

٤. حماية الشبكة ومنع انهيارها.

٥. قيادة العمليات النفسية والتقنية للمصادر.

الفصل السادس عشر

السيناريوهات التطبيقية المتقدمة

(Advanced Operational Scenarios)

يهدف هذا الفصل إلى تحويل المعرفة النظرية والمهارات العملية إلى خبرة تشغيلية فعلية من خلال سيناريوهات متعددة تغطي جميع المستويات HUMINT: التقليدي، HUMINT Cyber، الأمن الرقمي، والتحليل البيومتري. ويقصد به: القياسات الحيوية أو الخصائص البيولوجية المميزة للأفراد، والتي تُستخدم للتعرّف عليهم والتحقق من هويتهم. بصمة الأصابع.

بصمة العين (قزحية/شبكية) بصمة الوجه بصمة الصوت بصمة الكف الحمض النووي

السيناريو ١: تشغيل مصدر داخل مؤسسة حساسة

الموقف

مصدر داخلي يعمل داخل وزارة حكومية، يمتلك وصولًا لمعلومات حساسة تتعلق بمشروع استراتيجي. هناك مراقبة أمنية

مشددة وحظر استخدام الأجهزة الشخصية داخل مقر العمل.

خطوات التنفيذ

١. البحث والتحليل المسبق دراسة خلفية المصدر، بيئة العمل، الزملاء، الإجراءات الأمنية.

٢. الاقتراب الأولي لقاء اجتماعي بسيط خارج مقر العمل، للتأكد من استعداد المصدر للتعاون.

٣. بناء الثقة تقديم دعم معنوي وضمان حماية المصدر، مع تعليمات سرية واضحة.

٤. جمع المعلومات الأولية طلب معلومات عامة لا تضع المصدر تحت الخطر.

٥. تقييم المخاطر اليومية وضع خطة طوارئ للتعامل مع أي تفتيش أو مراقبة مفاجئة.

٦. التوسع التدريجي في المهام بعد التأكد من الالتزام والثقة، يمكن طلب معلومات أكثر حساسية.

المخرجات

١. شبكة موثوقة لمصدر داخل مؤسسة حساسة.

٢. خطة طوارئ واضحة للمخاطر المحتملة.

٣. سجل معلوماتي دقيق للتحليل لاحقًا.

السيناريو ٢: تجنيد إلكتروني داخل مجموعات مغلقة

الموقف

فتح خط تشغيل داخل مجموعة رقمية مغلقة (منتدى أو شبكة اجتماعية خاصة)، الهدف هو الوصول لمصادر معلومات ذات قيمة.

خطوات التنفيذ

١. إنشاء الهوية الرقمية (Digital Legend) ملف وهمي متكامل ينسجم مع بيئة المجموعة.

٢. الاندماج الاجتماعي الرقمي المشاركة بالمحتوى، بناء الثقة مع الأعضاء.

٣. المراقبة وجمع المعلومات: ملاحظة الأنشطة والتفاعلات، تحديد الأعضاء المحتملين للتجنيد.

٤. الاقتراب المباشر إرسال رسائل شخصية مختارة بعناية لتقديم عرض التعاون.

٥. إدارة الاتصال الرقمي استخدام قنوات مشفرة، وتدوين جميع التفاصيل بدون كشف الهوية.

٦. تحويل العضو إلى مصدر دائم تقديم محفزات، تعليمات واضحة، وخط خروج رقمي آمن.

المخرجات

١. مصدر رقمي مستقر وموثوق.

٢. خط اتصال مشفر وآمن.

٣. قدرة على إدارة المصادر الرقمية ضمن الشبكات المغلقة.

السيناريو ٣: تشغيل في بيئة عدائية عالية

الموقف

مصدر داخل جماعة معادية، البيئة مليئة بالمراقبة والخطر، الحاجة لمعلومات عاجلة خلال ٧٢ ساعة.

خطوات التنفيذ

١. تحديد المخاطر الأساسية نقاط التفتيش، كاميرات المراقبة، الأفراد ذوي النفوذ.

٢. تخطيط اللقاءات منخفضة الرؤية مواقع غير متوقعة، أوقات عشوائية لتجنب التتبع.

٣. استخدام التغطية الميدانية (Cover Story) تقديم سبب منطقي للوجود أو الاتصال.

٤. جمع المعلومات بطريقة آمنة صور، رسائل مشفرة، تسليم مباشر في نقاط محمية.

٥. إدارة الطوارئ خطوط خروج متعددة، تعليمات واضحة للتصرف في حالة كشف المصدر.

٦. التقييم الفوري مراجعة جودة المعلومات، إعادة ضبط العلاقة إذا لزم.

المخرجات

١. معلومات حساسة تم جمعها دون تعريض المصدر للخطر.

٢. خطة طوارئ فعّالة للتعامل مع أي تهديد مفاجئ.

السيناريو ٤: كشف تضليل داخلي في شبكة مصادر متعددة

الموقف

شبكة مصادر متعددة، بعض المصادر تقدم معلومات متناقضة، وهناك خطر تضليل متعمد أو غير متعمد.

خطوات التنفيذ

١. تحديد مصادر التضليل المحتملة تحليل التناقضات الزمنية، اللهجية، والمحتوى.

٢. جمع أدلة إضافية استخدام مراقبة مستقلة أو مصدر آخر للتحقق.

٣. إجراء مقابلات تقييمية للمصدر طرح أسئلة دقيقة بدون كشف الشكوك.

٤. إعادة توزيع المهام تصحيح التضارب بتوجيه المصدر بعيدًا عن المسار الحرِج.

٥. تطبيق الرقابة المتبادلة تأكيد المعلومات من خلال مصدر مستقل.

المخرجات

١. إزالة التضليل وتحسين جودة المعلومات.

٢. حماية مصداقية الشبكة بالكامل.

السيناريو ٥: تشغيل مزدوج(Source Double Operation)

الموقف

مصدر رئيسي يجب استخدامه لجمع معلومات من جهتين متناقضتين، مع الحفاظ على سلامة المصدر.

خطوات التنفيذ

١. تقييم المصدر التأكد من ولائه، قدرته على الفصل بين المهمتين.

٢. تحديد خطوط اتصال منفصلة لكل مهمة، قناة آمنة، توقيت مستقل.

٣. إعداد سيناريو التفاعل كيف يتصرف المصدر إذا تم اكتشافه أو وضع تحت ضغط.

٤. تقديم تحفيزات مزدوجة ضمان التزامه بالمهام دون خلق توتر أو شعور بالتهديد.

٥. مراقبة دقيقة متابعة كل خطوة وتسجيل كل المعلومات للمعالجة لاحقًا.

المخرجات

١. القدرة على إدارة عملية مزدوجة دون كشف المصدر.

٢. معلومات متعددة تدعم القرارات الاستخباراتية.

السيناريو ٦: تشغيل عبر الأجهزة المشفرة

الموقف

مصدر يستخدم أجهزة رقمية للوصول لمعلومات داخل بيئة مغلقة.

خطوات التنفيذ

١. تأمين الأجهزة تشفير حديث، استخدام VPN، حماية ضد البرمجيات الخبيثة.

٢. تحديد بروتوكولات الاتصال رسائل مشفرة، أوقات محددة للتواصل.

٣. جمع المعلومات ملفات، رسائل، بيانات حساسة بدون كشف الهوية.

٤. تقييم التهديد السيبراني مراقبة الهجمات المحتملة أو الاختراقات.

٥. تحديث الهوية الرقمية بشكل دوري لتقليل فرص كشف المصدر.

المخرجات

١. شبكة رقمية مؤمنة.

٢. حماية فعّالة لهوية المصدر وبياناته.

السيناريو ٧: مواجهة حادثة كشف مصدر داخل المؤسسة

الموقف

مصدر تم كشفه جزئيًا، المخاطرة عالية، يجب اتخاذ إجراءات عاجلة.

خطوات التنفيذ

١. تفعيل خطة الطوارئ إخراج المصدر من بيئة الخطر بسرعة.

٢. تقييم الضرر ما المعلومات التي تم كشفها؟ من يمكن أن يصل إليها؟

٣. إعادة ضبط الشبكة تعديل خطط التشغيل للمصادر الأخرى.

٤. إعادة بناء الثقة مع المصدر المتبقي لضمان استمرار التعاون.

المخرجات

١. الحد من الضرر الناتج عن الكشف.

٢. ضمان استمرار العملية بشكل آمن.

السيناريو ٨: تشغيل في بيئة متعددة الجنسيات

الموقف

مصادر تعمل ضمن بيئات دولية، قوانين مختلفة، مراقبة عالية، اختلاف ثقافي.

خطوات التنفيذ

١. تحليل البيئة القانونية والثقافية تجنب خرق القوانين المحلية.

٢. بناء علاقات محلية تفهم عادات المصدر وثقافته.

٣. إدارة الاتصالات الدولية خطوط مشفرة، توقيتات مختلفة حسب الدولة.

٤. جمع المعلومات متعددة الجنسيات تحليل البيانات وتحويلها إلى تقييم موحد.

المخرجات

١. معلومات دقيقة عبر بيئات متعددة.

٢. شبكة متوازنة آمنة قانونيًا وثقافيًا.

السيناريو ٩: التعامل مع مصادر عالية القيمة

(HVA – High Value Assets)

الموقف

مصدر يمتلك وصولًا لمعلومات استراتيجية حاسمة، الخطأ قد يكون كارثيًا.

طوات التنفيذ

١. تقييم شامل للمخاطر شخصيًا، بيئيًا، رقميًا.

٢. إعداد خطة حماية متعددة الطبقات مواقع آمنة، اتصالات مشفرة، تحفيزات مستمرة.

٣. جمع المعلومات بشكل تدريجي عدم الضغط على المصدر.

٤. مراقبة دقيقة استخدام فرق متعددة لمتابعة أي مؤشرات تهديد.

المخرجات

١. حماية مصدر استراتيجي.

٢. معلومات دقيقة تدعم القرار على أعلى مستوى.

السيناريو ١٠: تشغيل الشبكات متعددة الطبقات (Layered Source Networks)

الموقف

شبكة من ٣–٥ مصادر تعمل في طبقات مختلفة للوصول لمعلومة معقدة.

خطوات التنفيذ

١. تحليل الشبكة تحديد مصادر أساسية، ثانوية، احتياطية.

٢. إدارة الاتصال متعدد الطبقات منع اتصال المصادر ببعضها مباشرة.

٣. إعداد خط طوارئ لكل طبقة إجراءات محددة لكل مصدر في حال اكتشافه أو فشل مهمته.

٤. تقييم الأداء الدوري مراقبة جودة المعلومات وولاء كل مصدر.

٥. إعادة توزيع المصادر عند الضرورة مرونة عالية حسب تغير الوضع.

المخرجات

شبكة متينة ومستقرة.

١. جمع معلومات معقدة بأمان .

الفصل السابع عشر

النماذج والأدوات الاحترافية

(Operational Tools & Templates)

هذا الفصل يحتوي على أكثر من ٣٥ نموذجًا وأداة تشغيلية مصممة لتسهيل العمل الاستخباراتي ومنع الأخطاء البشرية، مع شروحات ومفاهيم دقيقة لكل نموذج.

القسم الأول: نماذج التقييم الأولي للمصدر

(Initial Source Evaluation Forms)

١. نموذج تقييم القابلية للتجنيد

(Recruitability Assessment Form)

الهدف : تحديد ما إذا كان الشخص مناسبًا للتجنيد.

المعايير:

المعيار | الوصف | الدرجة من ١٠|

: الدافع الأساسي – مالي - أيديولوجي - انتقامي - مهني.

: درجة الوصول – مستوى وصول الشخص للمعلومة المطلوبة.

: نقاط الضعف – هل يمتلك Vulnerabilities يمكن استخدامها؟

: مستوى المخاطر – حجمه، إمكانية كشف الوكيل، قانونية العملية

: السلوك العام – هدوء - اندفاع - ولاء - تردد.

: إمكانية السيطرة : هل يمكن السيطرة عليه بسهولة؟

التفسير

١. مجموع ≥ ٤٠ = مرشح ممتاز.

٢. مجموع ٢٥-٣٩ = تحت المراقبة.

٣. أقل من ٢٥ = غير مناسب.

٢. نموذج تقييم الثقة بالمصدر
(Source Reliability Rating – SRR)

المعايير الأساسية

١. مصداقية المعلومات السابقة.

٢. الانضباط.

٣. الاستجابة في المواعيد.

٤. عدم وجود تضارب.

٥. عدم المبالغة بالسرد.

٦. القدرة على الاحتفاظ بالسرية.

سلم التقييم

A = عالي جدًا.

B = جيد.

C = متوسط.

D = منخفض.

E = خطر/غير صالح.

٣. نموذج تقييم البيئة التشغيلية
(Operational Environment Assessment)

العناصر

١. مستوى الأمن في المنطقة.

٢. وجود كاميرات.

٣. نقاط تفتيش.

٤. احتمالات المراقبة الميدانية.

٥. حساسية المعلومات.

٦. احتمالية وجود مراقبة مضادة (Counter Surveillance) .

القسم الثاني: نماذج التشغيل اليومي
(Daily Operational Templates)

٤. نموذج جدول لقاءات منخفضة الرؤية
(Low-Visibility Meetings Table)

اليوم	الموقع	وقت الوصول	وقت المغادرة	قناة الطوارئ	ملاحظة أمنية

٥. نموذج خطة حماية المصدر
(Source Protection Plan – SPP)

عناصر الخطة

١. اسم رمز المصدر.

٢. تحليل المخاطر الشخصية.

٣. نقاط التهديد المحتملة.

٤. خطة خروج طارئة.

٥. خطة تغطية Story Cover .

٦. معدات أمنية للأزمات.

٧. جدول تواصل مشفر.

٦. نموذج تقييم المعلومات المستلمة
(Information Quality Evaluation – IQE)

رقم المهمة | النوع | درجة الحساسية | صحة المعلومة |
------------ ------------- ----- ---------

تضارب | مصدر داعم للمعلومة | التقييم النهائي|
---------- -------------- -----

٧. نموذج تحليل خطر كشف المصدر داخل المؤسسة
(Internal Leak Risk Analysis)

يتضمن:

١. تحديد الأشخاص الذين قد يشكون.
٢. سلوكيات يجب تجنبها.
٣. أوقات حساسة يجب تجنبها.
٤. أسلوب رد المصدر عند الاستجواب.

القسم الثالث: النماذج الرقمية(Cyber-HUMINT Forms)

٨. نموذج بناء الهوية الرقمية(Digital Legend Form)

يشمل:

١. الاسم الوهمي.
٢. الخلفية الاجتماعية.

٣. المهنة.

٤. طريقة الكتابة.

٥. اهتمامات متناسقة.

٦. المواقع المستخدمة.

٧. تبرير وجود الحساب.

٨. السيناريو الخلفي الكامل.

٩. نموذج تسجيل الأنشطة الرقمية للمصدر (Digital Activity Log)

|التاريخ | المنصة | نوع النشاط | الهدف | مستوى المخاطر | ملاحظة|

| --- | ----- | ------ | ---- | ---------- | ----- |

١٠. نموذج تقييم البصمة الرقمية (Digital Footprint Assessment)

يتضمن:

١. قوة كلمات المرور.

٢. وجود حسابات قديمة.

٣. أخطاء في الهوية الوهمية.

٤. علاقات غير ضرورية.

٥. احتمالات كشف الهوية.

القسم الرابع: نماذج الأمن والاستخبارات المضادة

(Counterintelligence Tools)

١١. نموذج كشف التضليل

(Disinformation Detection Checklist)

المعايير:

١. اختلافات زمنية.

٢. غياب الصور الداعمة.

٣. تضارب مع مصادر أخرى.

٤. مبالغة في التفاصيل.

٥. نمط لغوي غير معتاد.

٦. دوافع محتملة للكذب.

١٢. نموذج رصد مراقبة ميدانية

(Surveillance Detection Route – SDR)

يشمل:

١. نقاط توقف.

٢. تغييرات مفاجئة في الاتجاه.

٣. سلوكيات مشبوهة.

٤. سيارات أو أشخاص يتكرر ظهورهم.

١٣. نموذج تحليل الدوافع السلوكية للمصدر (Behavioral Motivation Matrix)

العوامل الخمسة الأساسية:

١. دافع مادي.

٢. دافع عاطفي.

٣. دافع نفسي.

٤. دافع سياسي.

٥. دافع انتقامي.

القسم الخامس: نماذج التخطيط العملياتي (Operational Planning Templates)

١٤. نموذج خطة العملية(Operation Plan – OPPLAN)

العناصر الأساسية:

١. الهدف النهائي للعملية.

٢. وصف البيئة.

٣. مصادر الدعم.

٤. مصادر التهديد.

٥. التسلسل الزمني.

٦. خطة الاتصال.

٧. خطة الطوارئ.

٨. خطة الانسحاب.

٩. خطة ما بعد العملية.

١٥. نموذج تقدير الموقف الاستخباراتي (Intelligence Estimate – IE)

يشمل:

١. الوضع العام.

٢. القدرات المعادية.

٣. النوايا المحتملة.

٤. الثغرات.

٥. تقدير المخاطر.

التوصيات

١٦. نموذج تحليل SWOT للمصدر

| العنصر | محتوى التحليل|

| ---- | ---------- |

| نقاط القوة

| نقاط الضعف

- الفرص
- التهديدات

القسم السادس: نماذج السيناريوهات
(Scenario Modeling Templates)

١٧. نموذج سيناريو تشغيل مصدر في بيئة عدائية

يتضمن:

١. شخصيات السيناريو.

٢. البيئة.

٣. مراحل اللقاء.

٤. التهديدات.

٥. نقاط الكسر.

٦. خطة النسخ الاحتياطي.

١٨. نموذج سيناريو تشغيل عبر الإنترنت
(Cyber Scenario Template)

يشمل:

١. طبيعة المجموعة.

٢. طريقة الاختراق.

٣. مراحل بناء الثقة.

٤. خطة التجنيد.

٥. أدوات الاتصال.

٦. مؤشرات الخطر.

١٩. نموذج سناريو تشغيل مزدوج

يشمل:

١. جهتين رئيسيتين.

٢. طريقة الفصل.

٣. خطة المناورة.

٤. تقييم الخطر.

٥. نقاط انكشاف محتملة.

القسم السابع: نماذج بيومترية وسلوكية

(Biometric & Behavioral Tools)

٢٠. نموذج تحليل الصوت(Voice Stress Analysis Log)

يشمل:

١. النبرة.

٢. الترددات.

٣. تغيرات الطابع الصوتي.

٤. مؤشرات القلق.

٥. مؤشرات الكذب.

٢١. نموذج تحليل لغة الجسد

(Body Language Decoding Sheet)

العناصر:

١. حركة اليدين.

٢. انحناء الظهر.

٣. اتجاه النظر.

٤. اهتزاز القدم.

٥. مسافة الأمان.

٢٢. نموذج نمط الاتصال السلوكي للمصدر

(Behavioral Communication Pattern)

يشمل:

١. طريقة الكلام.

٢. المفردات الأساسية.

٣. مدة الرد.

٤. التوتر.

٥. السرعة.

٦. التغيرات الطارئة.

القسم الثامن: نماذج إدارة شبكة المصادر

(Network Management Tools)

٢٣. نموذج تسجيل شبكة المصادر

(Source Network Registry)

كود المصدر	مستوى الوصول	مستوى المخاطر	آخر تقييم	نوع المهام	حالة التشغيل

٢٤. نموذج توزيع المهام بين المصادر

(Task Distribution Matrix)

المهمة	المصدر الأساسي	المصدر الاحتياطي	الزمن	أولوية	مستوى الحساسية

٢٥. نموذج تقييم تجانس الشبكة

(Network Harmony Evaluation)

يقيس

١. التناقض في المعلومات.

٢. مستوى الولاء.

٣. نقاط الاحتكاك.

٤. احتمالات الكشف.

القسم التاسع: نماذج الأمن الرقمي المتقدم

(Advanced Digital Security)

٢٦. نموذج خطة التشفير(Encryption Strategy Sheet)

يتضمن:

نوع التشفير

١. بروتوكول تبادل المفاتيح.

٢. دورة تغيير المفاتيح.

٣. خطة الطوارئ عند اختراق الجهاز.

٢٧. نموذج إدارة البصمة الرقمية للمصدر

١. الحسابات.

٢. الصور.

٣. الروابط.

٤. سجل المتابعة.

٥. نقاط الضعف الرقمية.

القسم العاشر: نماذج الطوارئ (Emergency & Crisis Forms)

٢٨. نموذج خطة الخروج الآمن (Emergency Exit Plan – EEP)

العناصر

١. نقطة الالتقاء.

٢. خطة بديلة.

٣. وسيلة اتصال.

شخص التواصل.

رمز الطوارئ.

٢٩. نموذج التعامل مع حادثة كشف
(Exposure Response Sheet)

يتضمن:

١. ما تم كشفه.

٢. من كشفه.

٣. مستوى الخطر.

٤. الإجراءات الفورية.

٥. إجراءات التخفيض.

٦. خطة الاستعادة.

٣٠. نموذج إدارة الوقت الحرج
(Critical Time Window Management)

يستخدم عند طلب معلومات خلال ٢٤-٧٢ ساعة .

القسم الحادي عشر: النماذج القانونية والأخلاقية
(Legal & Ethical Templates)

٣١. نموذج الامتثال القانوني (Legal Compliance Checklist)

١. هل تم الالتزام بالقانون المحلي؟

٢. هل هناك خطر دبلوماسي؟

٣. هل توجد مسؤولية جنائية محتملة؟

٤. هل يجب إبلاغ القيادة؟

٣٢. نموذج تقييم الأثر الأخلاقي للعملية
(Ethical Impact Review)

١. هل يتم استغلال المصدر بشكل مفرط؟

٢. هل العمل يهدد حياة غير معنين؟

٣. هل يوجد خط أحمر يجب احترامه؟

القسم الثاني عشر: نماذج التقارير (Reporting Templates)

٣٣. نموذج التقرير السري اليومي

(Daily Confidential Report – DCR)

يتضمن:

١. عنوان المهمة.

٢. ملخص سريع.

٣. المعلومة الخام.

٤. تقييم المعلومة.

٥. المخاطر.

٦. التوصيات.

٣٤. نموذج التقرير التحليلي النهائي

(Final Intelligence Report – FIR)

يتضمن:

١. مقدمة.

٢. معلومات خام.

٣. تحليل معزز بالأدلة.

٤. تقييم احتمالات.

٥. اتخاذ القرار.

توصيات نهائية

٣٥. نموذج تقرير تقدير المخاطر (Risk Assessment Report)

يشمل:

١. مستوى الخطر.

٢. احتمالية الحدوث.

٣. شدة الأثر.

٤. خطة المعالجة.

٥. المراقبة.

امثلة قريبة من الواقع لعمليات اتخاذ بيوت امنة وعمليات تجنيد عملاء

التقارير المتوفرة لأغراض التدريب

تقرير استخباراتي خاص للغاية

البيوت الآمنة الفائقة السرية التابعة لجهه مخابراتية داخل دولة قابلة للاختراق، المخصصة لاختراق دائرة مسؤول عالي المستوى.

البيت رقم (١) ـ الاسم الرمزي: منزل العنكبوت.

موقع المنزل (تحديد دقيق نسبيًا):

اسم البلد محافظة ٠٠٠ - قضاء ٠٠٠ - حي ٠٠٠

قرب شارع "٣٣"، خلف "العيادة الخاصة "VIP" التابعة لمؤسسة من مؤسسات المجتمع المدني.

المنزل مموّه على أنه مجمّع استشارات قانونية تابع لمحامي سابق في سلك القضاء.

الوظيفة الأساسية للمنزل:

هذا ليس بيتًا اعتياديًا، بل مركز استخبارات ميداني تقني متطور يُستخدم في:

- التنصت السلبي على إشارات الاتصالات الخاصة بمكتب المسؤول رفيع المستوى عبر تحليل الترددات المنخفضة (VLF/UHF).
- اعتراض وتحليل بثّ الاتصالات المغلقة الصادرة عن سيارات الحماية المصفحة (من نوع خاص).
- تشغيل خوادم مرآة مرتبطة بأنظمة قيادة وسيطرة داخل مؤسسات الحمايات الخاصة بالمسؤول، مستغلة ثغرات زرعها من قبل الجهه المخابراتية المعادية في عمليات تقنية سابقة.
- تحليل أنماط الإرسال الزمني لرسم خريطة حركة المسؤول وأقرب مستشاريه دون الحاجة لتتبّع مباشر.

الهيكل الداخلي للمنزل:

- الطابق الأرضي: صالة استقبال وهمية، وغرفـة اجتماعـات لا تُستخدم إلا للتغطية.
- الطابق السفلي الأول: مركز خـوادم يضـم ١٢ وحـدة تخـزين تعمل على نظـام مشـفر يطلـق عليـه فـي مخـابرات الجهـه المستفيدة اسم بيت الزيبق.
- الطابق السفلي الثاني (محجـوب عـن التصـاريح الرسـمية): يحتوي على وحدة تحليل إشـارات رقميـة، وأجهـزة SDR، ومنظومة بث مزدوج (Relay Echo).

العملاء المحوريون المرتبطون بالمنزل:

١, – ٠٠٠٠٠ وهو مجند تم تجنيدة ويمكن الاعتماد علية

١. مواليد: ١٩٨٢-المنشأ: محل الولادة من تولد نفس سكان المحافظة.

٢. الغطاء: أستاذ جامعي في جامعة معروفـة -يعمـل فـي قسـم الأمن السيبراني.

٣. المهام: تركيب البرمجيات الأساسية لمنظومـات الاختـراق، وتوجيه البيانات نحو خوادم خارجية عبر أنفاق مشفّرة.

٤. ملاحظات أمنية: يُعتقد أنه تدرّب في احدى الدول وحصل على شهادة عالية في التخصص ٢٠١١ تحت غطاء دورة أكاديمية.

٢. العميل (١١١١١١)

١. مواليد: ١٩٧٦ ـ المنشأ: من نفس البلد.

٢. الغطاء: رجل أعمال يملك شركة اتصالات مرخصة في العاصمة تم تجنيده مسبقا.

٣. المهام: نقل وتركيب أجهزة الاتصالات ذات التقنية العالية، وربطها مع منظومات خارجية.

٤. ملاحظات أمنية: يستخدم جواز سفر ثانٍ باسم مستعار" عند السفر إلى دولة اخرى.

تحليل استخباراتي عالي المستوى:

- يتم تصنيف هذا المنزل ضمن فئة "منازل الظل المحرّم" داخل بنك أهداف وحدة الجهه المستفيدة.
- يعد هذا الموقع طرفًا في مشروع خاص يُعرف داخل مؤسسات مخابرات الجهه المستفيدة باسم:

بيت العنكبوت

والذي يهدف إلى إنشاء نسخة رقمية خفية من الروتين الأمني والسياسي مسؤول رفيع المستوى، دون اختراق مادي مباشر.

●يعتمد المنزل على تقنية تعرف.

بـ Echo-Mimicry Protocols لتوليد بيانات مرآة تنقل إلى موقع ثالث خارج هذا البلد، ثم تعاد إلى وحـدات تحليـل فـي دولة الجهه المستفيده.

توصيات أمنية للوقاية:

١. إجراء مسح إشاري (Signal Sweep) أسبوعي فـي محـيط مكتب المسؤل المقصود بالهدف.
٢. كم، باستخدام أجهزة كاشف إشارات من نوع. HIL-٦٥٠٠ .
٣. إغـلاق جميـع الاتصـالات غيـر الضـوئية ضـمن تحركـات المسـؤول، وتحويـل كـل الاتصـالات إلـى قنـوات ضـوئية (Fiber Secured).
٤. زرع مصادر بشرية داخل المؤسسات التقنيـة الجامعيـة ذات الصلة بالمخابرات، خصوصًا "جامعة الأستاذ العميل الاول" و "جامعة وجامعة اخرى".
٥. منع عمليات صيانة كاذبة فـي المنـاطق المحاذيـة لمقـرات القيادة المركزية، خصوصًا تلك التـي تـتم بواسـطة سـيارات إسعاف خاصة أو شركات تنظيف مغمورة.

تقرير ثاني لأغراض التدريب

البيت يسمى((بيت الجوكر)) اساسي

تقرير استخباراتي مفصل عن البيت الآمن "بيت الجوكر" - في منطقة وسط عاصمة الدولة.

الرمز: بيت آمن رقم ٠٠١ - "الاسم الوهمي(بيت الجوكر).

الموقع الجغرافي الدقيق:والوصف

يقع بيت الجوكر" في شارع ٢٣ تقاطع شارع ١٠، حي النسر في العاصمة. المبنى عبارة عن فيلا سكنية متماسكة مكونة من ثلاث طوابق، ذات واجهة حجرية تقليدية مزخرفة تحيط بها أسوار عالية يبلغ ارتفاعها ٣٫٥ متر، مزودة بكاميرات مراقبة متقدمة تغطي كل الاتجاهات، مع بوابة كهربائية مزدوجة مؤمنة بأنظمة قفل ذكية (رموز رقمية وبصمة إصبع).

البنية التحتية والتجهيزات:

- الهيكل: فيلا حجرية مبنية مع أساسات قوية مضادة للاهتزاز، تحوي غرفاً متعددة مخصصة للاجتماعات، غرف تشغيل ومراقبة، غرف تخزين سرية تحت الأرض.
- الغرف: غرفة مركزية للاجتماعات سعتها تصل إلى ١٥

شخصًا مجهزة بنظام صوتي مشفر وأجهزة عرض مخفية.

- التخزين: غرفة سرية تحت الأرض مغلقة بأبواب فولاذية مقاومة للاختراق، تحتوي على خزائن إلكترونية لحفظ الوثائق والأرشيف والوسائط الرقمية المشفرة.
- الاتصالات: مجهز بأحدث أجهزة الاتصال المشفرة، منها محطة اتصال فضائي خاصة متصلة بأقمار صناعية، بالإضافة لأجهزة لاسلكية تعمل بترددات منخفضة ضد الرصد.
- الأمن الإلكتروني: نظام تشفير مزدوج الطبقة (AES-٢٥٦ وRSA-٢٠٤٨) لجميع البيانات الواردة والصادرة، مع استخدام جدران نارية متقدمة وأنظمة كشف التسلل السيبراني.
- المراقبة: شبكة كاميرات CCTV داخلية وخارجية متصلة بمركز مراقبة يعمل ٢٤/٧، مع أنظمة كشف حركة متقدمة ومجسات صوتية.

خطط الطوارئ والأمان:

- غرفة هروب سرية: مخرج طوارئ مخفي يؤدي إلى شبكة أنفاق مهجورة تحت احد الاحياء، يسمح بالخروج السريع في حالات الاقتحام أو المداهمة.

- تدمير سريع للأدلة: نظام إلكتروني متقدم يسمح بتدمير الوثائق والأجهزة الحساسة خلال أقل من ٣ دقائق عبر غرف مخصصة.
- إنذار مبكر: مجسات حركة وكاميرات حرارية مرتبطة بنظام إنذار ينبه فريق التدخل السريع لدى مخابرات الدولة المهدفة تلقائيًا.
- التشويش الإلكتروني: عند تنشيط خطة الطوارئ، تُفعّل أجهزة تشويش لمنع التنصت أو اعتراض الاتصالات في محيط البيت.

الموظفون والعاملون:

- المشرف الرئيسي: ١٢٣رمز للاسم الوهمي ، مهندس اتصالات سابق، مسؤول عن تأمين خطوط الاتصال، الصيانة التقنية، والإشراف الأمني.
- عملاء داعمين:

١ ك ي ع، موظف في وزارة الداخلية، مسؤول عن تسهيل نقل المعلومات.

٢ ج د ق، مختص بالدعم اللوجستي وتأمين الوثائق المزورة.

وظائف البيت الأساسية:

- مركز اجتماعات استخباراتية سرية.
- نقطة تخزين آمنة للوثائق والأجهزة الرقمية الحساسة.
- قاعدة عمليات لوجستية لتنسيق مهام التجسس والعمليات الميدانية.
- مركز مراقبة وتواصل مباشر مع العملاء الميدانيين.

تحليل نقاط القوة والضعف:

- نقاط القوة: موقع مركزي داخل العاصمة مع بنية تحتية متطورة وخطوط اتصال مشفرة ومراقبة صارمة.
- نقاط الضعف: كثافة الوجود الأمني والميليشيات في العاصمة قد تعرض البيت لخطر المداهمة أو الرصد إذا تم الكشف عن الموقع.
- اعتماد كبير على التكنولوجيا المتقدمة التي يمكن أن تكون عرضة لشن هجمات سيبرانية أو تشويش.
- الوحدة المسؤولة: الوحدة ٠٠٠٠٠ (وحدة الاستخبارات التقنية) التابعة للمخابرات المهدفة.

خطط الطوارئ:

في حال تعرض البيت لأي تهديد، هناك نظام إخلاء سريع عبر مخرج سري في الطابق الأرضي يؤدي إلى شبكة أنفاق مهجورة. النظام الأمني يسمح بحجب أي اتصالات إلكترونية داخل وخارج البيت تلقائياً. يوجد مخبأ مؤقت للوثائق الحساسة بعيداً عن البيت يدار من قبل فريق دعم متنقل في المنطقة.

تحليل خطوط الاتصال:

البيت يتصل مباشرة مع ٣ بيوت آمنة رئيسية في مناطق داخل العاصمة عبر قنوات مشفرة تعتمد على أجهزة اتصال لاسلكي متطورة ومحطات إرسال خفية داخل المباني. تبادل المعلومات يتم عبر رموز سرية وبروتوكولات متعددة الطبقات لتجنب التعقب.

بيت امن اخر كمثال

تقرير استخباراتي مفصل عن بيت "الصقر الأسود" – منطقة وسط العاصمة

العنوان التفصيلي:

شارع ٠٠٠٠٠، بناية رقم ٢٧، الدور الثاني، قرب تقاطع شارع اسم وهمي.

الوصف:

بيت متوسط المساحة، مخفي بين عمارات سكنية قديمة، تم تجديده بشكل سري ليشمل تجهيزات تقنية متقدمة للمراقبة والتواصل. مزود بنظام كاميرات حرارية وأجهزة إنذار بيومترية تستخدم بصمة العين للولوج إلى الغرف الحساسة. يحتوي على غرفة مركزية لتحليل المعلومات والوثائق مع خط اتصال مشفر إلى مركز القيادة.

المشرف الرئيسي على البيت:

العميل الرمزي: "اسم مستعار ٠٠٠٠"

- الاسم الكامل: ------------- .
- اسم الأب: -------------- .
- أول حرف من اسم: --------- .
- المهنة: موظف حكومي سابق في وزارة الاتصالات.
- التحصيل الدراسي: شهادة دبلوم في تقنية المعلومات من معهد ؟؟؟؟؟؟ التقني.
- موقعه الحالي: اسم العاصمة حي------------ .

- طريقة التجنيد: تم استقطابه عام -------- عبر اتصال غير مباشر مع عميل للمخابرات خلال مناسبة اجتماعية.
- الأعمال المنجزة: إدارة شبكة الاتصالات الرقمية للبيت، توفير الدعم الفني لتشفير البيانات وإرسالها.
- استخدام البيت: مركز لجمع البيانات الاستخباراتية وتخزينها مؤقتاً، نقطة توزيع معلومات للمشغلين الميدانيين.
- طرق التمويه: تغطية البيت كمقر جمعية خيرية محلية، أنشطة ظاهرية اجتماعية لتفادي الشكوك.
- طرق الوقاية: نظام أمني متعدد الطبقات يشمل تعقبات إلكترونية لمنع التنصت، إجراءات دخول صارمة تعتمد على التحقق البيومتري.
- طرق كشف العميل: تحليل اتصالاته الرقمية ونمط استخدامه للإنترنت، مراقبة تحركاته الفعلية وتغييراته المفاجئة في الروتين.
- الوحدة هيه الوحدة التقنية الرقمية في المخابرات الدولة المهدفة (الوحدة) ٠٠٠٠٠

خطط الطوارئ:

الوصف العام للبيت

يحتوي البيت على غرفة آمنة داخلية مقاومة للانفجارات، مع نظام قفل إلكتروني منفصل. في حالة تعرض البيت لأي خطر، يتم تفعيل آلية قفل أوتوماتيكي مع إخطار مباشر لمركز القيادة. المخرجات السرية تؤدي إلى نفق مائي تحت الأرض يصل إلى نهر دجلة، مما يسمح بالإخلاء السريع والمخفي.

تحليل خطوط الاتصال:

هذا البيت يشكل نقطة محورية في شبكة الاتصالات الداخلية حد الاجهزه المعاديه داخل العراق داخل العراق، يرتبط بشكل مباشر بمركز القيادة في عاصمة الجهاز المعادي عن طريق قنوات مشفرة معتمدة على أقمار صناعية خاصة، بالإضافة إلى استخدام أجهزة بث لاسلكي عالية التردد داخل بغداد للتواصل مع بيوت آمنة أخرى، ما يضمن السرية والتواصُل السريع والآمن.

تجنيد ضابط

تم التحفظ لكونه تقرير تدريبي

الاسم بلا

الرتبة: ضابط.

الموقـع: قسـم مكافحـة التجسـس - جهـاز الأمـن او جهـاز استخباراتي.

المسؤوليات الرسمية: مسؤول عـن مراقبـة أنشـطة التجسـس داخل هذا الجهاز تحديد التهديدات الأمنية، وإجـراء التحقيقـات مع المشتبه بهم.

خلفية شخصية وتعليمية:

العمر: حوالي ٥٠ سنة.

المؤهل العلمي: حاصل على شهادة بكالوريوس في الهندسة الإلكترونية من جامعة (------)، بدرجة ماجستير فـي الأمـن المعلوماتي (---------) .

الخلفية العائلية: ينتمي إلى عائلـة ذات نفـوذ متوسـط ومـن سـكان عاصـمة هـذه الدولـة، يعـاني مـن ضـغوط ماليـة بسـبب متطلبات أسرته الكبيرة وبحاجة الى تامين وضع مادية يـتلائم مـع الظروف والظغوط التي يعيشها.

طريقة التجنيد:

تــم اســتدراجه عــام ٢٠١٥ مــن قبــل عناصــر احــد أجهــزة المخابرات التابعة لدولة معادية لدولته أثناء سفره إلى دولة مجاورة لإجراء دورات تدريبية في مجال الأمن السـيبراني. اسـتغل جهـاز المخابرات المهدف ضعف موقفه المالي وحاجتـه لـدعم أسـرته، وقدم له عرضًا مغريًـا للمـال والتـأمين. تـم تدريبـه علـى تقنيـات التواصل المشفر والتعامل مع أنظمة استخباراتية معقدة تسبق هذه التدريبات عمليـات لقـاءات متكـررة وتقـديم مغريـات لاقناعـة واختبارة بموافقة العمل.

طبيعة العمل والاستخبارات:

يوفرلجهاز المخـابرات المهـدف تقـارير سـرية منتظمـة عـن عمليات مكافحة التجسس التي ينفذها جهاز الأمن التابع لدولته، مما يمكن لجهاز المخابرات المهدف من معرفة خطوات الكشف والتتبع التي تقوم بها هذه الدولة ضد العملاء والمخترقين.

يسرب أسـماء وشـفرات عمليـات سـرية، ويقـدم تحـديثات دورية عن استراتيجيات الدفاع الإلكتروني.

دوره حيوي فـي تعطيـل جهـود جهـاز الأمـن التـابع لـه مـن الداخل عبر توفير معلومـات حاسـمة تسـمح لجهـاز المخـابرات

المهدف بإعادة ترتيب تحركاتها والابتعاد عن المناطق المكشوفة.

أساليب الاتصال:

يعتمد على قنوات اتصال مشفرة عبر شبكة الإنترنت باستخدام برمجيات معقدة (VPN + TOR) .

يتم اللقاء به شخصياً في مواقع سرية بعيداً عن العاصمة لضمان السرية.

يستخدم شبكة من الوسطاء لنقل المعلومات إلى جهات الاتصال المخابراتية المهدفة.

يستخدم أجهزة اتصالات متنقلة مزيفة مغطاة بأجهزة تقطيع الإشارة لتفادي التعقب.

العنوان والبيت الآمن الخاصة بالضابط المجند:

البيت الآمن: شقة فاخرة في ضاحية شمال العاصمة، رقم ١٢، بلوك ٥، ضمن مجمع سكني راقي.

تم تجهيز البيت بأنظمة مراقبة داخلية وخارجية متطورة، مع إمكانيات تشويش إلكتروني عالية المستوى لمنع التنصت أو الاختراق.

المنزل محاط بدائرة أمنية خاصة تضم عناصر مدربة للحماية وحراسة فنية مكثفة.

أبرز العمليات الناجحة:

ساعد في إفشال محاولات جهازه الامني لكشف شبكة التجسس للدولة المهدفة عام ٢٠١٩ عبر تسريب تقارير داخلية تم تعديلها بشكل يسمح الجهاز المعادي بالتحكم في الموقف.

ساهم في إبطال عملية أمنية كانت تستهدف عملاء محلين تابعين للمخابرات المهدفة، مما أتاح لهم الفرار وتجنب اعتقالات واسعة.

نقل معلومات استخباراتية أدت إلى تعرية عملية تهريب أسلحة كانت تستهدف الدولة المهدفه، ما مكّن الجهاز المعادي من اتخاذ إجراءات مضادة.

تقنيات التجنيد النفسي - كيف يختاراي جهاز مخابراتي متطور عملاءه ويتحكم بهم؟

يُعد تجنيد العملاء أحد الأعمدة المركزية في عمل الجهاز المعادي، ويُدار بأساليب نفسية دقيقة مبنية على فهم عميق للبشر ودوافعهم. لا يعتمد الجهاز المعادي فقط على المال أو التهديد، بل يُجيد اللعب على الحاجات العاطفية، الإيديولوجية، والنفسية للأهداف المراد تجنيدها. تبدأ العملية بدراسة موسعة للشخص، ثم بناء علاقة بطيئة، وتنتهي بالسيطرة الكاملة عليه فكريًا أو نفسيًا.

مرحلة الدراسة والتحليل النفسي

- تُجمع معلومات من المصادر المفتوحة والمراقبة الميدانية.
- يتم تحديد نقاط الضعف: المال، الطموح، الشعور بالرفض، الرغبة في الانتقام.
- تُستخدم تقنيات تحليل الشخصية لتقييم قابلية الهدف للتجنيد.

مرحلة الاختراق الاجتماعي

- يدخل عميل المخابرات (المجند) في حياة الهدف تدريجيًا.
- قد يبدأ الأمر بعلاقة صداقة، أو دعم مهني، أو حتى ارتباط عاطفي.
- يُمنح الهدف شعورًا بالأهمية، والاهتمام، والانتماء.

مرحلة عرض التعاون

- يتم تقديم التعاون كفرصة أو خدمة، وليس كخيانة.
- تُستخدم عبارات مشوشة لغويًا: 'مساعدة في الأمن الدولي مراقبة نشاطات عدائية.'
- يُشعر الهدف بأنه ما يزال في الجانب الأخلاقي أو الوطني.

مرحلة الربط النفسي والسيطرة

- بعد أول مشاركة للمعلومات، يتم خلق حالة 'لا عودة.'
- يتم تعميق العلاقة، وتقديم مكافآت أو حماية.
- تُستخدم عناصر الابتزاز الناعم أو التبعية النفسية لمنع الانشقاق.

أنواع الأهداف المفضلة لدى الموساد

نوع الشخصية	الصفات المستهدفة	الأسلوب المناسب للتجنيد
الشخص الطموح غير المُقدّر	يريد إثبات نفسه ويشعر بالتجاهل	المديح، الدعم الوظيفي، الاستقطاب المالي
الشخص الغاضب من النظام	ناقم على الدولة أو المؤسسة	الإقناع الإيديولوجي، إثارة مشاعر الانتقام
الوحيد اجتماعيًا	يبحث عن علاقات واعتراف خارجي	العلاقات العاطفية أو الصداقة العميقة
الانتهازي النفعي	يركز على الفوائد المادية والمنافع	الإغراء المالي والتسهيلات المعيشية

الخاتمة

التجنيد النفسي ليس فقط عملية استخباراتية، بل هو فن دقيق يعتمد على علم النفس والسلوك الإنساني. قدرة الجهاز المعـادي على قراءة الأفراد والسيطرة عليهم تكمن في صبره، ودقتـه، وفهمـه العميق للعقل البشري.

مثال / تقرير اسـتخباراتي - وحـدة الصـقر الابـيض (وحـدة التنصّت الدولي).

التعريف بالوحدة(وحدة التنصت الدولي)

- الاسم الرمزي ((الصقر)).
- المهمـة الأساسـية: تنفيـذ عمليـات التنصّـت الإلكترونـي والفيزيائي على الاتصـالات الدوليـة، بمـا يشـمل التنصـت علـى الخطـوط الهاتفيـة، الأقمـار الصـناعية، الشـبكات الفضائية، وأنظمة الإنترنت العالمية.

الهيكل التنظيمي

- فرق متخصصة في التنصت على الاتصالات السلكية واللاسلكية.

- وحدات فرعية للتحليل والاستخلاص الاستخباراتي من البيانات المجمعة.
- فرق تقنية متقدمة مختصة بتطوير أدوات التنصت والاختراق.

أساليب العمل والتقنيات

- التنصت عبر الأقمار الصناعية وبرامج التجسس المعقدة.
- اختراق شبكات الاتصالات الدولية باستخدام برمجيات خبيثة وتسلل مستمر (APT).
- استخدام محطات تنصت متقدمة على الأرض وفي البحر وفي الفضاء.
- تحليل بيانات الاتصالات الصوتية، المرئية، والبيانية لاستخلاص معلومات استخباراتية حيوية.

أهداف الوحدة

- مراقبة الاتصالات الدبلوماسية والعسكرية.
- جمع معلومات استخباراتية اقتصادية وسياسية.
- رصد تحركات الجهات المعادية والمنظمات الإرهابية عبر الاتصالات.
- دعم عمليات التخريب السيبراني والهجمات الإلكترونية الموجهة.

طرق الوقاية من وحدة الصقر (وحدة التنصّت الدولي)

١. تشفير الاتصالات

١. اعتماد بروتوكولات تشفير قوية مثل (TLS ١٫٣، AES-٢٥٦) لجميع وسائل الاتصال الصوتي، النصي، والبياني.

٢. استخدام شبكات VPN آمنة ومصممة خصيصًا لمواجهة التنصت المتقدم.

٢. المراقبة المستمرة

١. تحليل دوري لحركة الشبكة لاكتشاف محاولات التنصت أو التسلل.

٢. نشر أنظمة كشف التسلل (IDS) وأنظمة منع التسلل (IPS) مع تحديث مستمر.

٣. حماية الأجهزة والمعدات

١. تأمين الأجهزة المستخدمة في الاتصالات ضد برامج التجسس والاختراق.

٢. فحص دوري للأجهزة للكشف عن أي أجهزة تنصت مادية أو برمجية.

٤. استخدام خطوط اتصال خاصة

١. إنشاء خطوط اتصال مغلقة خاصة (مثل الشبكات المغلقة Air-gapped) للاتصالات الحساسة.

٢. الاعتماد على الأقمار الصناعية أو قنوات الاتصالات المشفرة الخاصة.

٥. التدريب والتوعية الأمنية

١. تدريب العاملين على التعامل الآمن مع الاتصالات واستخدام الأجهزة المشفرة.

٢. نشر ثقافة أمنية صارمة لمنع التسريبات أو الاستخدام الخاطئ للأجهزة.

٦. إدارة الوصول والتحكم

١. تطبيق مبدأ الأقل امتيازًا في منح الصلاحيات لاستخدام أنظمة الاتصال.

٢. اعتماد المصادقة متعددة العوامل (MFA) للوصول إلى الأجهزة والشبكات.

٧. إجراءات مكافحة التجسس

١. إجراء فحوصات أمنية دورية لتحديد وجود أجهزة أو برامج تنصت.

٢. اعتماد بروتوكولات تعقيم إلكتروني لتطهير الأجهزة من البرامج الخبيثة.

٧. التحكم في بيئة العمل

١. فرض سياسات صارمة لمنع دخول الأجهزة غير المصرح بها إلى مناطق العمل.

٢. إنشاء مناطق محمية ومراقبة بشدة للاتصالات الحساسة.

طرق الوقاية التفصيلية من وحدة الصقر الابيض (وحدة التنصّت الدولي)

١. تشفير شامل ومتحرك للبيانات

١. تطبيق تشفير نهاية إلى نهاية (E٢EE) لجميع أنواع الاتصالات (صوت، نص، فيديو، بيانات).

٢. استخدام تقنيات التشفير الديناميكية التي تتغير مع كل جلسة اتصال لمنع فك التشفير المستمر.

٢. شبكات خاصة ومعزولة

١. إنشاء شبكات خاصة افتراضية (VPN) بتشفير عالي، مع إعدادات خاصة لمنع تسرب DNS أوIP .

٢. اعتماد الشبكات المغلقة (Air-gapped Networks) في

نقل المعلومات الحساسة حيث لا تكون متصلة بالإنترنت.

٣. تقنيات الكشف عن التنصت

١. تركيب أجهزة وأنظمة كشف التنصت الإلكتروني (مثل أجهزة كشف تداخل الإشارات أو الاختراق).

٢. مراقبة حركة المرور الشبكية لاكتشاف محاولات التنصت أو الاختراق أو الإرسال غير المصرح به.

٤. حماية الأجهزة المادية

١. فحص الأجهزة المستخدمة في الاتصالات بشكل دوري للكشف عن أجهزة تنصت أو شرائح تجسس مخفية.

٢. استخدام أجهزة مشفرة ومتقدمة مصممة لمنع التسلل واكتشاف البرمجيات الخبيثة.

٤. تحديث البرامج والأنظمة باستمرار

١. اعتماد سياسة تحديث مستمر للبرمجيات وأنظمة التشغيل لمنع استغلال الثغرات الأمنية.

٢. استخدام جدران نارية متقدمة وبرمجيات مكافحة الفيروسات المتخصصة.

٥. إدارة الهوية والوصول

١. تطبيق المصادقة متعددة العوامل (MFA) لجميع المستخدمين.

٢. تنفيذ مبدأ أقل امتياز (Least Privilege) في منح الصلاحيات للوصول إلى أنظمة الاتصالات.

٦. توعية وتدريب العاملين

١. تنفيذ دورات تدريبية منتظمة لرفع مستوى الوعي الأمني حول مخاطر التنصت.

٢. تعليم التعامل السليم مع البيانات الحساسة وطرق استخدام أدوات التشفير.

٧. مراقبة وتحليل مستمر للأنشطة

١. إنشاء مراكز عمليات أمنية (SOC) لرصد وتحليل الأحداث والأنشطة المشبوهة.

٢. استخدام أنظمة تحليل متقدمة تعتمد على الذكاء الاصطناعي للكشف المبكر عن التنصت.

٨. تقييد استخدام الأجهزة الشخصية

١. منع استخدام الأجهزة الشخصية غير المعتمدة في مناطق العمل الحساسة.

٢. فرض سياسات صارمة على استخدام الهواتف المحمولة وأجهزة التخزين.

٩. التعاون مع خبراء أمن سيبراني

١. إجراء مراجعات أمنية واختبارات اختراق دورية من قبل خبراء خارجيين.

٢. تطبيق توصيات أمنية حديثة باستمرار لمواجهة تطور تقنيات التنصت.

بناء ملفات عمليات تجنيد لأغراض التدريب وتبيان محاولات عملية الاختراق

١. الملف الببغاء الافريقي: اسم وهمي

الهوية الاستخباراتية: بلا

١. الاسم الرمزي الكامل: الببغاء الافريقي( ) .

٢. الرتبة: عقيد في جهاز الرقابة والتفتيش - قسم مكافحة الاختراق الأجنبي.

٣. الوظيفة: مسؤول المراجعة الأمنية الدورية على مقرات الأجهزة الاستخباراتية والامنية في جميع المحافظات.

٤. الغطاء الرسمي: مفتش أمني.

٥. العمر التقريبي: ٤٧ سنة.
٦. الرمز الداخلي في قاعدة "بيتا (بلا ------).

التحليل الاستخباراتي السلوكي:

الخلفية:

٧. خدم سابقًا في أجهزة الدولة قبل انتقاله إلى الملف الأمني بعد حادثة اختراق داخلي فشلت عام ٠٠٠٠ في احد المحافظات.
٨. يملك سمعة صارمة داخل النظام الحكومي، لكنه معروف بأسلوبه البيروقراطي البطيء.
٩. لا يُؤخذ عليه ميل مالي واضح، إلا أنه شخصية انطوائية وسهلة العزل الذهني عن المحيط.

مؤشرات القابلية للاختراق:

١٠. يمر بأزمة نفسية منذ وفاة ابنه الأكبر حيث تعرض لحادثة اغتيال ضمن عمله وقد ألقى باللوم غير المعلن على إدارة العمليات التي يعمل فيها.
١١. عززت تلك الأزمة قناعته بـ"فقدان القيمة الحقيقية لما يفعله"، وهو تعبير استخدمه في جلسة خاصة تمت مراقبتها صوتيًا في فندق حيث كان في اجتماع عائلي ويحظره بعض المقربون.

أصبح معزولًا تدريجيًا من باقي طاقم الرقابة، ويُقال إنـه يكتـب تقاريره الأخيرة بناءً على اجتهاده الشخصي لا بناءً على التعليمات.

تفاصيل عملية الاختراق:

المرحلة الأولى – التوجيه النفسي:

١. تم تشخيص حالته من قبل وحدة أبحاث نفسية في مخابرات دولة مهدفة لأغـراض عمليـة التجنيـد أواخـر --------- للعام بعد اعتراض إلكتروني لرسائله الشخصية المشفرة مـع ابنته المقيمة في احدى الدول الاوربية.

٢. تم بناء نموذج نفسي له عبـر منصـة مراقبـة سـلوكية باسـم " (--------) تعتمـد علـى تحليـل لغـوي دقيـق لأنمـاط الإحباط والانكسار.

المرحلة الثانية – الاتصال الهادئ:

٣. تلقى فبراير لسنة(-------) رسالة منسوبة إلـى "جمعيـة أســر الشــهداء او المتظـررين جـراء العمليـات الارهابيـة المغتربين"، تتضمن دعوة رمزية لحضور مؤتمر فـي احـدى الدول، تم الترتيب له عبر وسيط مقرب منه.

٤. المؤتمر لم يكن حقيقياً، بل وسيلة لإقناعه بتبادل "ملفات أمان إقليمي" تخص تقارير أمنية مزورة عن احدى الدول المجاورة لبلده مقابل تقديم وثائق "أخلاقية" عن فساد قيادات في مؤسسات عسكرية في بلده.

المرحلة الثالثة – التسريب المقنن:

٥. استُدرج إلى تسريب ثلاث دفعات من تقارير التدقيق الأمني على مقار احد الأجهزة الأمنية العسكرية التابة لبلده في منطقة خارج مدينته التي يسكنها، تحتوي على:

١. مواقع أجهزة المراقبة.

٢. أسماء العناصر التي خضعت للتحقيق الداخلي خلال الأشهر الستة السابقة.

٣. رموز التحذير المبكر للضباط المصنفين كـ"عرضة للاختراق."

التقييم الأمني:

نوع الاختراق الذي تم التسلل من خلاله هو نفسي وأخلاقي، وليس عبر حوافز مالية.

مقدار الضرر المعلوماتي الـذي أحدثـه متوسـط فـي الوقـت الحالي، لكنه يحمل خطورة متزايدة في المستقبل بسبب حساسية المعلومات التي تسربت.

درجة سيطرته على الملفات حساسة ومهمة ولكنها متوسـطة؛ حيث يملك وصولًا جزئيًا إلى وثائق وتقارير حيوية.

إمكانية كشفه أو فضحه داخليًا منخفضة للغايـة، ممـا يجعـل من الصعب على اجهزة الامن الداخلي التعرف على اختراقه.

حاليًـا، هـو فـي حالـة نشـاط مسـتمر ولكـن تحـت مراقبـة استخباراتية من بعيد.

الملف ١١٢٢: (م) (لشمس الساطعة).

الهوية الاستخباراتية:

- الاسم الرمزي الكامل: أبو الهول (----------) .
- الرتبة: مقدم.
- المنصب: قائد وحدة مراقبة الاتصالات والمراقبة الإلكترونيـة داخل جهاز الأمن.
- الغطـاء الرسـمي: مسـؤول قسـم التحليـل التقنـي فـي مركـز الاتصالات التابع لجهاز الأمن الداخلي.

- مكان العمل: مقر الجهاز الأمني المركزي عاصمة الدولة.
- العمر: حوالي ٥٠ سنة.
- الرمز الداخلي في قاعدة البيانات.

الخلفية المهنية والشخصية:

- يمتلك خلفية تقنية قوية، حيث درس الهندسة الإلكترونية في جامعة ام الهول التحق بجهاز الأمن الفيدرالي في قسم الاتصالات.
- معروف بذكائه العالي ومهاراته التقنية المتقدمة، ما جعله محورًا رئيسيًا في مراقبة الاتصالات المشفرة والرقمية.
- شخصيته هادئة، متحفظة، ويميل إلى العزلة رغم تواجده في موقع قيادي تقني حساس.
- يعاني من ضغوط متكررة بسبب طبيعة عمله التي تتطلب يقظة دائمة، مما أدى إلى اضطرابات نوم متكررة وميل للتوتر المزمن.

العوامل النفسية التي أثرت عليه:

- شهد انفصالًا عائليًا صعبًا قبل عامين أدى إلى عزلته الاجتماعية وتراجع معنوياته.

- تُظهر تحليلات سلوكية من خلال تتبع نشاطه الرقمي إشارات إلى استياء متزايد من الإدارة وعدم الثقة بالقيادات العليا.
- ظهر في مراسلات مشفرة مهتمة بموضوعات الحريات الشخصية والضغوط النفسية، وهو ما استُغل لاحقًا كمدخل للتواصل معه من جهات استخباراتية معادية.

المرحلة الأولى: جمع المعلومات وبناء الملف النفسي

- تم جمع معلومات دقيقة عن حياته الشخصية والعملية من خلال اختراقات أمنية سابقة لشبكته المنزلية وأجهزة اتصاله الخاصة.
- استُخدمت هذه المعلومات لإعداد ملف نفسي مفصل يكشف عن نقاط ضعفه في العلاقات الاجتماعية والضغوط النفسية.

المرحلة الثانية: الاقتراب عبر الوسائل التقنية

- تم التواصل معه عبر تطبيقات مراسلة مشفرة استخدمت كغطاء لجهات استخباراتية أجنبية لاستقطابه تدريجياً.
- عُرضت عليه "فرص عمل استشارية تقنية" في الخارج مع وعود بدعم نفسي ومادي، الأمر الذي جذب اهتمامه في ظل وضعه النفسي.

المرحلة الثالثة: تسريب المعلومات التقنية

- بدأ بتسريب معلومات تقنية عن أنظمة مراقبة الاتصالات داخل احد الأجهزة المهمة تشمل:

١. تفاصيل تشفيرية لأنظمة الاتصالات السرية.

٢. نقاط ضعف في البرمجيات المستخدمة في مراقبة الاتصالات.

٣. جداول ترددات الإشارات ومواعيد تفريغ المعلومات.

- التسريبات تمت بشكل ذكي ومحسوب، بحيث لا تثير الشكوك الفورية، مع إخفاء آثار الاتصال عبر شبكات خاصة افتراضية (VPN) ورموز معقدة.

التقييم الأمني الكامل:

- نوع الاختراق: نفسي وتقني، يعتمد على الضغط النفسي والتلاعب بظروفه الشخصية.
- مدى الضرر المعلوماتي: مرتفع، خاصة على الصعيد التقني، لما يشكله من اختراق في أنظمة الاتصالات الحساسة.
- درجة السيطرة على المعلومات: عالية، حيث يتحكم في بيانات حيوية تتعلق بالبنية التحتية للمراقبة الإلكترونية.
- إمكانية كشف الاختراق داخليًا: متوسطة، بسبب الطبيعة التقنية المعقدة للتسريبات وصعوبة تتبعها.

- الوضع الحالي: مستمر في أداء مهامـه، لكـن مراقـب بشـكل دقيق من قبل فرق أمنية متخصصة.
- نقطـة الضـعف الاسـتراتيجية: الضـغوط النفسـية والعزلـة الاجتماعية التي يعاني منها، مما يجعل التعامـل معـه نقطـة حرجة في تأمين الشبكة الداخلية.

الملف ٠٠ ٠٠٠: هامون (ع) - ((''الصنم'')).

الهوية الاستخباراتية:

- الاسم الرمزي الكامل:وهو اسم مستعار وهمي((هامون)).
- الرتبة: عميد.
- المنصب: رئيس قسم الاستخبارات العسـكرية فـي فـي احـد الأجهزة الامنية، مسؤول تنسـيق المعلومـات الاسـتخباراتية العملياتية بين فروع الأجهزة المختلفة.
- الغطاء الرسمي: قائد مركز الاسـتخبارات التكتيكيـة فـي مقـر القيادة.
- مكان العمل: عاصمة الدولة، مقر القيادة العامة.
- العمر: حوالي ٥٧ سنة
- الرمز الداخلي في قاعدة البيانات (بلا------).

الخلفية المهنية والشخصية:

- خدم في مؤسسات الدولة منذ أوائل الثمانينيات، وشارك في حروب عدة- حيث برز كقائد ميداني متمكن.
- تدرج في المناصب الاستخباراتية حتى وصل لرئاسة قسم الاستخبارات العسكرية، ويُعتبر من أقوى وأذكى الضباط في الجهاز.
- معروف بسلوكه الحازم وقدرته على اتخاذ قرارات سريعة وحاسمة، مع شبكة علاقات واسعة داخل وخارج المؤسسات التي عمل فيها.
- يمتاز بشخصية مركبة تجمع بين الكاريزما والصرامة، وقدرته على إدارة ملفات حساسة وصعبة بكفاءة عالية.
- يعاني من ضغوط سياسية داخلية بسبب تنافس نفوذ بين أجنحة المؤسسات الامنية المختلفة، مما جعله في موضع حساس للغاية.

العوامل النفسية التي أثرت عليه:

- يتمتع بثقة عالية بنفسه وذكاء حاد، لكن الضغوط المستمرة على مستوى القيادة تؤثر أحيانًا على توازنه النفسي.
- تظهر تقارير مراقبة سلوكية مؤشرات على توتر دائم، وعزلة شبه تامة عن المحيطين به، مع ميل لعدم الثقة بأي جهة

سوى دائرة ضيقة جدًا من المقربين.

- لديه حساسية مفرطة تجاه أي محاولات استغلال نفوذه أو التلاعب به، ويُعتقد أنه يتعامل بحذر شديد مع موظفيه.

تفاصيل عملية الاختراق:

المرحلة الأولى: الاستهداف الاستخباراتي المكثف

- تم استهدافه عبر جهازين مختلفين: جهة استخباراتية معادية تعمل على اختراق مؤسسته، وجهاز منافس داخلي ضمن هذه المؤسسة يحاول تقويض مكانته.
- استُخدمت عدة طرق تجمع بين جمع معلومات شخصية ومالية، ورصد تفاعلاته مع بعض الجهات الخارجية.

المرحلة الثانية: محاولة زرع عميل في محيطه

- نجحت جهة معادية جزئيًا في زرع عميل تحت غطاء موظف إداري قريب من دائرة ((هامون))، كان هدفه خلق ثغرات في نقل المعلومات الحساسة.
- هذا العميل نقل معلومات محدودة لكنها استراتيجية، مثل مواعيد اجتماعات استخباراتية سرية وأسماء ضباط مختارين.

المرحلة الثالثة: استغلال نقاط الضعف النفسية والسياسية

- استُغل تنافس النفوذ داخل المؤسسة لإثارة خلافات وتحريك دعاية داخلية تستهدف تقويض ثقة هامون في القيادة العليا.
- تعرض لضغوط من أطراف داخلية لتغيير توجهاته أو تسريب بعض التقارير الداخلية مقابل دعم سياسي أو حماية.

المرحلة الرابعة: محاولة الاختراق التقني المحدود

- بالرغم من خبرته الأمنية العالية، تم استهداف أجهزته الشخصية بهجمات إلكترونية متطورة عبر فيروسات مبرمجة خصيصًا لاختراق أنظمة الحماية الشخصية، لكنها لم تُحقق نجاحًا كاملاً.
- تم كشف هذه المحاولات مبكرًا واحتواء الخطر عبر فرق الأمن السيبراني.

التقييم الأمني الكامل:

- نوع الاختراق: مركب، نفسي وسياسي مع محاولات تقنية.
- مدى الضرر المعلوماتي: منخفض حتى الآن بسبب قدرة ((هامون)) على إدارة المخاطر، لكنه يشكل تهديدًا على مستوى النفوذ السياسي والاستخباراتي داخل مؤسسته.

- درجة السيطرة على المعلومات: محدودة، لأن معظم المعلومات الحساسة لا تزال محصنة بشكل جيد.
- إمكانية كشف الاختراق داخليًا: عالية، حيث يتلقى دعمًا مكثفًا من أجهزة الأمن السيبراني والاستخباراتي.
- الوضع الحالي: في حالة يقظة مستمرة، مع مراقبة محكمة لكل تحركاته وبيئته.
- نقطة الضعف الاستراتيجية: النزاعات الداخلية والضغوط السياسية، التي قد تؤثر على استقراره النفسي وسلامة قراراته.

الملف ٠٠ ٤٤: أبو سمره (ج) - "الجبل العالي".

الهوية الاستخباراتية: بلا

- الاسم الرمزي الكامل: أبو سمرة (الجبل العالي).
- الرتبة: لواء.
- المنصب: معاون قائد في الشؤون الأمنية والاستخباراتية.
- الغطاء الرسمي: مسؤول الأمن الداخلي والتنسيق الاستخباراتي مع الأجهزة الأمنية الأخرى.
- مكان العمل: مقر القيادة العامة لشؤون العمليات.
- العمر: حوالي ٤٩ سنة.
- الرمز الداخلي في قاعدة البيانات: (بلا ------) .

الخلفية المهنية والشخصية:

- من أقدم الضباط الذين قضوا أكثر من ٢٥ سنة في صفوف العمليات، شارك في العديد من العمليات العسكرية والاستخباراتية داخليًا وخارجيًا.
- حاصل على تدريب استخباراتي متقدم في مؤسسات أمنية خارجية مرتبطة بشؤون العمليات الخارجية، لديه خبرة واسعة في عمليات مكافحة التجسس.
- شخصية صارمة وصارمة جداً، ومعروف بمستوى ولائه العالي لحكومته، ويُعتبر من أبرز المدافعين عن الخط الأمني
- معروف بحرصه الشديد على السرية، ويتعامل بحذر مع كل معلوماته وأجهزته، مما يجعل اختراقه صعبًا للغاية.

العوامل النفسية التي أثرت عليه:

- يتمتع بثقة عالية بالنفس وقوة تحمل، لكنه يعاني من ضغوط نفسية ناتجة عن مسؤولياته الثقيلة والمخاطر التي يتعرض لها يوميًا.
- يميل للعزلة المهنية ويُفضل العمل مع دائرة ضيقة من الموثوقين، مما قد يعرضه لمحاولات استغلال العزلة.
- تقارير استخباراتية تشير إلى توتر متزايد بسبب التحديات

الأمنية المتصاعدة في المنطقة، مما يؤثر على استقراره النفسي.

تفاصيل عملية الاختراق:

المرحلة الأولى: استهداف عميق ومعقد

- خضع لمراقبة مكثفة من جهات استخباراتية معادية، حاولت جمع معلومات من خلال شبكات التواصل الخاصة به والعلاقات المهنية.
- تم رصد عدة محاولات لاستغلال علاقاته الخارجية، خصوصًا مع بعض ضباط مؤسسته المتقاعدين الذين قد يكونون أكثر عرضة للاستغلال.

المرحلة الثانية: محاولة زرع عميل ثانوي

- تم إدخال عنصر استخباراتي كموظف دعم لوجستي داخل قسمه الأمني، هدفه الوصول إلى معلومات حساسة حول خطط الحرس.
- لم يُكشف هذا العميل إلا بعد فترة طويلة، وقد ساهم في نقل بعض المعلومات غير الجوهرية لتجنب كشفه بسرعة.

المرحلة الثالثة: هجمات إلكترونية متقدمة

- استُهدفت أجهزته الشخصية والمحمولة بمحـاولات اختـراق عبر برمجيات تجسس متطورة، لكن الحماية التقنية العاليـة حالت دون أي تسرب معلوماتي خطير.
- استخدمت البرمجيات تقنيات تشويش وتضليل لتغطية أثرهـا، ولكن فرق الأمن السيبراني نجحت في إحباط الهجمات.

التقييم الأمني الكامل:

- نوع الاختراق: استغلال علاقات مهنية ونفسية مـع محـاولات تقنية.
- مدى الضرر المعلوماتي: منخفض نسبيًا، حيث لـم تتسـرب معلومات حساسة مهمة.
- درجة السيطرة على المعلومات: جيـدة، مـع اسـتمرار جهـود مراقبة دقيقة.
- إمكانية كشف الاختراق داخليًا: متوسـطة إلـى عاليـة، بفضـل الحصانة الأمنية.
- الوضع الحالي: في حالـة تأهـب دائـم، مـع إجـراءات أمـان مشددة على كافة المستويات.

- نقطة الضعف الاستراتيجية: العزلة الاجتماعية والاعتماد الكبير على دائرة محدودة من الموظفين، مما قد يفتح ثغرات إذا استغلها العدو.

ملحق رقم ٢

الكــراس المتخصــص فــي التحليــل النفســي والفســلجي والباراسيكولوجي لانتخاب وإدارة المصادر الاستخباراتية الحديثة

ملاحظـة مهمـة: هـذا الكـراس معـد للأغـراض الأكاديميـة والتدريبية فقـط. جميـع الأمثلـة محايـدة وقانونيـة، ويركـز علـى منهجية علمية لتقييم الشخصيات وتحليلها قبل التعامل كمصـادر استخباراتية.

الفصل الأول: مقدمة علمية وأمنية

١. مفهــوم الانتخــاب النفســي للمصــادر: دراســة الســمات النفسية والسلوكية لاختيار الأشخاص المناسبين كمصادر موثوقة.

التعريف: هــو دراســة الســمات النفســية والســلوكية للأفــراد بهدف تحديد الأشخاص الأكثر ملاءمة ليكونوا مصادر معلومات موثوقة، مع التركيز على القدرات الذهنية، الانضباط، والمصداقية.

مثال: عند اختيار موظف لتقديم معلومات عن نشاطات مالية مشبوهة داخل شركة، يقوم المحلـل النفســي بتقيـيم ســماته مثـل

الانتباه للتفاصيل، الضمير المهني، وقدرته على التعامل مع ضغط العمل دون كذب أو تهرب.

٢. أهميـة التحليـل الفسـلجي والسـلوكي: قـراءة الجسـد، الإيماءات، والتغيرات الفسيولوجية كمؤشرات للصدق أو التوتر .

التعريف: هو استخدام مراقبة الجسد، الإيمـاءات، وتغيـرات الوظـائف الفسـيولوجية (مثـل ضـربات القلـب، التعـرق، تعـابير الوجه) كمؤشرات على صدق الشخص أو وجود توتر أو خداع.

مثال: خلال مقابلة مـع مصـدر محتمـل، يلاحـظ المحلـل أن المصدر يتعرق بشدة أو يتجنب النظر مباشرة عند الإجابة عن أسـئلة حساسة، ما قد يشير إلى شعوره بالتوتر أو محاولة إخفاء معلومات.

٣. تاريخ الدراسة الأكاديمية والتطبيقيـة: تطـور علـم تحليـل الشخصية في مجالات الأمن والاستخبارات.

٤. المنهجيـة العلميـة: دمـج النظريـات النفسـية مـع أدوات القياس الميدانية والتقنيات الرقمية الحديثة.

التعريف: هي دمج النظريات النفسـية المعتمـدة مـع أدوات القياس الميدانية والتقنيات الرقميـة الحديثـة، مثـل الاسـتبيانات، المقـابلات المنظمـة، والتسـجيلات الرقميـة، لضـمان تقيـيم موضوعي ودقيق للمصادر.

مثال: إعداد تقييم شامل لمصدر محتمل باستخدام استبيان نفسي، مراقبة تفاعله في مقابلة مباشرة، وتحليل حركاته وسلوكه عبر برنامج رقمي للتعرف على المؤشرات الدقيقة للصدق والتوتر.

الفصل الثاني: الإطار العلمي والنظري

١. التحليل النفسي (Psychological Analysis) نظريات فرويد، يونغ، والسلوكية، مع التركيز على دوافع الفرد وانفعالاته:

التعريف: هو دراسة شخصية الفرد ودوافعه وانفعالاته بناءً على نظريات علم النفس مثل فرويد (اللاوعي والدوافع الأساسية)، يونغ (الأنماط النفسية والوظائف النفسية)، والمدارس السلوكية (التعلم والعادات). الهدف هو فهم ما يحرك سلوك الشخص واتجاهاته.

مثال: عند تقييم موظف محتمل ليصبح مصدرًا معلوماتيًا، يستخدم المحلل النفسي استبيانات لقياس القيم والمحفزات الداخلية للشخص، مثل ميله للكتمان أو الاستقامة، لتحديد مدى ملاءمته كمصدر موثوق.

٢. التحليل الفسلجي (Physiological Analysis) دراسة استجابات الجسم والسلوكيات غير للفظية أثناء المقابلات.

التعريف: هو دراسة استجابات الجسم غير الإرادية أثناء المقابلات، مثل تعابير الوجه، نبض القلب، التعرق، وحركات اليدين، بهدف كشف التوتر أو الكذب أو الانفعال الداخلي.

مثال: خلال مقابلة مع مصدر محتمل، يلاحظ المحلل أن المصدر يرفع كتفيه أو يتململ عند سؤال حساس، ما قد يدل على توتر أو محاولة إخفاء معلومة.

٤. الباراسيكولوجيا (Parapsychological Analysis)

استخدام الحدس والتحليل غير المباشر للميول والنوايا، ضمن حدود قانونية:

التعريف: استخدام الحدس والتحليل غير المباشر لميول الفرد ونواياه، مثل قراءة أنماط الكلام، نبرة الصوت، أو سلوكيات غير مباشرة، مع الالتزام بالحدود القانونية والأخلاقية.

مثال: يعتمد المحلل على شعوره وخبرته لملاحظة تناقضات دقيقة بين ما يقوله المصدر ولغة جسده، لتقدير مدى صدقه، دون انتهاك خصوصيته أو القانون.

التكامل بين الثلاثة: لتقديم صورة شاملة للمصدر قبل الانتخاب أو التجنيد. التكامل بين الثلاثة.

التعريف: الجمع بين التحليل النفسي والفسيولوجي

والباراسيكولوجي لإعطاء صورة شاملة ودقيقة عن المصدر قبل اتخاذ قرار بالانتخاب أو التجنيد، بحيث يتم تقييم الشخصية والسلوك والاستجابات الفطرية كلها معا.

مثال: قبل قبول شخص كمصدر، يجمع الفريق بين: استبيانات تحليل الشخصية، مراقبة استجابات جسده أثناء مقابلة، واستخدام خبرة المحلل في قراءة العلامات غير المباشرة، لتحديد مدى موثوقيته وكفاءته.

الفصل الثالث: المؤشرات النفسية للمصدر

١. الدوافع النفسية طموح، انتقام، انتماء، مصلحة مادية أو فكرية.

التعريف: هي الأسباب الداخلية التي تحفز الشخص على التصرف بطريقة معينة أو تقديم معلومات، مثل الطموح الشخصي، الرغبة في الانتقام، الانتماء لمجموعة، أو المصلحة المادية أو الفكرية.

مثال: عند مقابلة مصدر محتمل، يكتشف المحلل أن الدافع الرئيسي للشخص هو الفضول الفكري لمعرفة معلومات استخباراتية، وليس المكافأة المالية، مما يجعله مناسبًا كمصدر يعتمد على الحافز الفكري.

٢. سمات الشخصية المناسبة انضباط، اتزان، قدرة على الصبر والتحكم بالعاطفة.

التعريف: هي الخصائص النفسية والسلوكية التي تجعل الشخص موثوقًا كمصدر، مثل الانضباط، الاتزان النفسي، القدرة على الصبر، والتحكم بالعاطفة تحت ضغط العمل.

مثال: موظف يمتلك القدرة على عدم الانفعال عند مواجهة أسئلة حساسة أو ضغط ميداني، ويستطيع التفكير بهدوء قبل الإجابة، يعد مناسبًا كمصدر معلوماتي.

٣. مؤشرات المخاطر النفسية ازدواجية السلوك، اضطرابات انفعالية، ميل للكذب.

التعريف: هي العلامات التي تشير إلى أن الشخص قد يكون غير موثوق أو يشكل خطرًا على سلامة جمع المعلومات، مثل ازدواجية السلوك، اضطرابات انفعالية، أو ميل للكذب والخداع.

مثال: مصدر يظهر تناقضات مستمرة بين أقواله وأفعاله، أو ينفعل بسرعة عند مناقشة مواضيع حساسة، قد يمثل خطرًا في جمع المعلومات الدقيقة.

٤. اختبارات عمليةMMPI ١٦PF، تحليل الميول والدوافع.

التعريف: أدوات علمية لتقييم الشخصية والدوافع والميول، مثل:

MMPI (Minnesota Multiphasic Personality Inventory):
لتقييم الاضطرابات النفسية وأنماط الشخصية.

١٦PF (١٦ Personality Factors): لتحديد السمات الأساسية للشخصية.

تحليل الميول والدوافع: لتقدير ما يحفز الشخص على العمل كمصدر.

مثال: إجراء اختبار ١٦ PF لشخص محتمل لتحديد مدى تحمله للضغط، قدرته على التركيز، ومستوى الانضباط الشخصي قبل اتخاذ قرار بتجنيده كمصدر.

مثال تطبيقي تحديد مصدر يتمتع بدافع فكري مقابل مصدر ذو دافع مادي خلال المقابلة الأولى.

الوصف: خلال المقابلة الأولى، يمكن للباحث التمييز بين

مصدر ذو دافع فكري: يركز على المعرفة والفهم واكتساب المعلومات.

مصدر ذو دافع مادي: يكون اهتمامه الأساسي بالمكافأة المالية أو المصلحة الشخصية.

التطبيق: بناءً على هذا التمييز، يتم تحديد نوع المعلومات التي يمكن الحصول عليها ومدى موثوقية المصدر في المدى الطويل.

الفصل الرابع: التحليل الفسلجي للمصدر

١. القراءة الجسدية: حركة العين، تعبيرات الوجه، معدل التنفس، توتر العضلات

التعريف: هي مراقبة واستنتاج الحالة النفسية للشخص من خلال حركات جسده المختلفة، مثل حركة العينين، تعبيرات الوجه، معدل التنفس، توتر العضلات، ونبرة الصوت، لتقدير الصدق أو التوتر أو الانفعالات الداخلية.

مثال: عند سؤال مصدر محتمل عن معلومات حساسة، يلاحظ المحلل أن الشخص يرمش بسرعة أو يشد فكيه، ما قد يشير إلى توتر داخلي يحاول إخفاءه.

٢. الملاحظة الميدانية كيفية رصد التغيرات الدقيقة أثناء المقابلة.

التعريف: هي تقنية مراقبة دقيقة للتغيرات الصغيرة في سلوك الشخص أثناء المقابلة، مثل حركات اليدين، تغيرات في النبرة الصوتية، أو تعديل وضعية الجسم، بهدف كشف مؤشرات غير لفظية عن الانفعال أو الكذب.

مثال: المصدر يغير جلسته فجأة عند طرح سؤال حساس، ما قد يدل على شعوره بالضغط أو محاولة التهرب من الإجابة.

٣. أدوات بسيطة تحليل الصوت، مؤشرات اليدين، لغة الجسد.

التعريف: هي وسائل عملية لمراقبة وفهم السلوك الفسلجي، تشمل:

تحليل الصوت (نبرة الكلام، سرعة التحدث).

مؤشرات اليدين (حركات التوتر أو التردد).

لغة الجسد (وضعية الجسم، تعابير الوجه).

مثال: يستخدم المحلل صوت المصدر لتحديد التوتر، فارتفاع نبرة الكلام عند الإجابة عن سؤال معين يدل على انفعال غير معلن.

العلاقة مع الحالة النفسية ارتباط المؤشرات الفسلجية بالمزاج والانفعالات.

التعريف: هي الربط بين المؤشرات الفسلجية والمزاج أو الانفعالات الداخلية للشخص، بحيث تساعد قراءة الجسد على فهم الحالة النفسية الحقيقية، سواء كانت توتر، ارتياح، خوف، أو حماس.

مثال: ارتفاع معدل التنفس، شد العضلات، وتجنب النظر المباشر يمكن أن يشير إلى توتر المصدر، حتى إذا كان يتحدث بثقة ظاهرية.

مثال تطبيقي: ملاحظة ارتفاع معدل التنفس كدليل على توتر غير معلن.

الوصف: خلال مقابلة ميدانية، لاحظ المحلل أن معدل تنفس المصدر ارتفع فجأة عند سؤال عن معلومات حساسة، رغم أنه لم يُظهر أي علامات لفظية للتوتر.

الاستنتاج: هذه الإشارة الفسلجية تعتبر دليلًا على توتر غير معلن، ما يستدعي متابعة واستراتيجيات دقيقة في التعامل معه.

الفصل الخامس: التحليل الباراسيكولوجي

١. الإدراك فوق الحسي (ESP) تقدير دوافع المصدر من سلوك غير لفظي.

لإدراك فوق الحسي(ESP - Extra Sensory Perception)

التعريف: هو القدرة على إدراك أو استنتاج نوايا ودوافع الشخص من خلال إشارات غير لفظية دقيقة، مثل النغمة الشعورية في صوته، تسلسل حركاته، أو التفاعل اللاواعي مع الأسئلة، دون الاعتماد على الكلمات فقط.

يُستخدم في المجال الاستخباراتي لتقدير الميول والمواقف الخفية لدى المصدر.

مثال: خلال مقابلة، يشعر الضابط أن المصدر يتحدث بثقة مبالغ بها عند مناقشة موضوع معين، رغم أن لغة جسده (تراجع جسدي بسيط وتجنب النظر) تشير إلى تحفظ داخلي، ما يدل على أنه يخفي جزءًا من الحقيقة.

٢. الحدس الاستخباراتي قراءة أنماط السلوك واتجاهات القرار.

التعريف: هو القدرة على قراءة أنماط السلوك واتجاهات القرار عبر الخبرة والتجربة المتراكمة، بحيث يستطيع المحلل تكوين "إحساس مهني" حول مدى صدق أو خطورة الشخص حتى قبل ظهور مؤشرات مباشرة.

مثال: من خلال خبرته الطويلة، يلاحظ المحلل أن المصدر يتحدث بطريقة منمقة جدًا ويكرر العبارات الرسمية — مما يولّد "حدسًا استخباراتيًا" بأنه يحاول تلميع صورته للحصول على مكاسب لاحقة.

٣. تطبيقات عملية تقدير احتمالية تعاون المصدر أو مخاطر الانسحاب. التطبيقات العملية.

التعريف: استخدام التحليل الباراسيكولوجي لتقدير:

احتمالية تعاون المصدر: مدى استعداده النفسي للتعاون بصدق.

مخاطر الانسحاب: احتمال تراجع المصدر أو تغيّر موقفه في المستقبل نتيجة خوف أو ضغط نفسي.

مثال: بعد مقابلات عدة، يستنتج الضابط أن المصدر متردد ومتأثر بعلاقاته السابقة، ما يشير إلى احتمالية انسحاب عالية، فيوصي بعدم الاعتماد عليه كمصدر أساسي.

٤. حدود البارا سيكولوجيا استخدام الحدس فقط كعامل مساعد وليس أساسي في اتخاذ القرار.

التعريف: يجب استخدام الحدس والتحليل فوق الحسي كعامل مساعد في اتخاذ القرار، وليس كأداة رئيسية؛ لأن التقديرات الحدسية قد تتأثر بالعوامل الشخصية أو المواقف السابقة، وبالتالي تحتاج إلى دعم علمي أو سلوكي واضح قبل الاعتماد عليها.

مثال: إذا شعر المحلل بأن المصدر غير صادق، فلا يعتمد فقط على هذا الإحساس، بل يُجري مقابلة إضافية، ويقارن النتائج مع مؤشرات فسيولوجية وسلوكية قبل اتخاذ قرار نهائي.

مثال تطبيقي تقييم مصداقية المصدر عبر التوافق بين لغة الجسد وكلامه المعلن مثال تطبيقي.

الوصف: أثناء مقابلة ميدانية، يُلاحظ أن لغة جسد المصدر (ثبات النظر، نبرة الصوت المستقرة) تتوافق مع مضمون كلامه المعلن، مما يعزز الحدس بصدق نواياه.

أما إذا وُجد تناقض بين كلامه وثقته الجسدية، فذلك يُعد مؤشرًا مبكرًا على عدم المصداقية أو التلاعب.

الفصل السادس: أدوات التقييم المتكاملة

| الأداة | الاستخدام | ملاحظات|

| ------------ | -------- ||

|نماذج تقييم الشخصية | قياس الصفات النفسية الأساسية | معتمدة أكاديميًا|

|مؤشرات الفسلجية | قراءة الجسد والسلوك | لتقدير الانفعالات والصدق|

|جداول الباراسيكولوجيا | تحليل الحدس والنوايا | دعم القرار وليس أساسه|

الفصل السابع: المنهج العملي لتجنيد المصادر

١. الاقتراب الأولي تحليل المعلومات المتاحة عن المرشح.

التعريف: هي المرحلة الأولى في عملية تجنيد المصدر، وتشمل جمع وتحليل المعلومات المتاحة عن المرشح قبل أي تواصل مباشر. يتم التركيز على خلفيته الاجتماعية، مهنته، ارتباطاته، وسلوكياته العامة، لتحديد مدى ملاءمته وتقدير نقاط القوة والضعف.

مثال: قبل مقابلة موظف في مؤسسة حساسة، يقوم المحلل بجمع بياناته من المصادر المفتوحة (وسائل التواصل، بيئة العمل، الدائرة الاجتماعية) لتحديد إن كان منضبطًا، طموحًا، أو لديه مشاكل مالية يمكن أن تؤثر على موثوقيته.

٢. الملاحظة: دراسة السلوك غير اللفظي والمؤشرات الفسلجية.

التعريف: هي متابعة ودراسة السلوك غير اللفظي والمؤشرات الفسلجية أثناء المقابلة الأولى، مثل تعبيرات الوجه، نبرة الصوت، حركات اليد، والتغير في نمط التنفس. الهدف هو فهم مدى صدق الشخص واستعداده للتعاون.

مثال: خلال اللقاء، يلاحظ المحلل أن المرشح يتحدث بثقة عند مناقشة أمور عامة، لكنه يتجنب النظر ويغير نبرة صوته عند السؤال عن جهات اتصاله، ما يشير إلى تحفظ أو إخفاء معلومة.

٣. بناء الثقة التواصل المهني، وضوح الأهداف، احترام الحدود.

التعريف: عملية تدريجية تهدف إلى إنشاء علاقة مهنية قائمة على الاحترام والشفافية الجزئية، من خلال وضوح الهدف، الالتزام بالحدود الأخلاقية، وإظهار تقدير لقدرات المرشح.

الهدف هو تقليل الحذر النفسي وتحفيز التواصل الصادق

مثال: يتحدث الضابط مع المصدر المحتمل حول موضوعات عامة قريبة من اهتماماته دون ضغط مباشر، ما يجعله يشعر بالارتياح ويبدأ بمشاركة معلومات أولية من تلقاء نفسه.

٤. الاختبار النفسي استخدام اختبارات قصيرة لتقييم الشخصية والدوافع.

التعريف: هو تطبيق أدوات مختصرة لقياس السمات النفسية والدوافع، مثل اختبار "الميول والدوافع" أو استبيان الثقة والانضباط، لتقدير درجة الاستقرار النفسي والصدق في السلوك.

مثال: يُطلب من المرشح الإجابة على مجموعة من الأسئلة السريعة لتحديد مدى اندفاعه، تفكيره العقلاني، وميله إلى المغامرة، مما يساعد في رسم ملف نفسي دقيق عنه.

٥. التحفيز والتقييم تكييف أسلوب التعامل مع نوع الشخصية.

التعريف: المرحلة النهائية، وتشمل اختيار أسلوب التحفيز الأنسب (فكري، مادي، اجتماعي) بناءً على نوع الشخصية، ثم تقييم الأداء خلال اللقاءات اللاحقة لتحديد مدى التزام المصدر واستمراريته.

مثال: إذا تبيّن أن المصدر يسعى للتقدير والاعتراف أكثر من المال، يُحفَّز بإشراكه في نقاشات مهنية وتقدير مساهمته المعرفية، ما يعزز ولاءه واستقراره النفسي.

الفصل الثامن إدارة العلاقة مع المصدر

١. الحفاظ على استقرار المصدر النفسي.

التعريف: هي عملية مستمرة تهدف إلى ضمان بقاء المصدر في حالة نفسية مستقرة، خالية من التوتر المفرط أو الخوف، كي يتمكن من أداء مهامه بفعالية ودون فقدان الثقة.

تشمل هذه العملية المتابعة الدورية، تقليل الضغوط، ومعالجة أي شعور بالتهديد أو الشك.

مثال: يُلاحظ على أحد المصادر علامات قلق متزايدة بعد مهمة ميدانية، فيقوم الضابط بعقد لقاء غير رسمي معه، يشرح فيه أهمية أمانه الشخصي، ويُعيد تأكيد الثقة المتبادلة، مما يعيد له الاطمئنان والاستقرار.

٢. متابعة التغيرات السلوكية والفكرية.

التعريف: تتضمن مراقبة سلوك المصدر وأفكاره بشكل مستمر لرصد أي تبدلات في الولاء، المزاج، أو طريقة التفكير، والتي قد تعكس ضغوطًا نفسية أو تأثيرات خارجية.

مثال: بدأ المصدر مؤخرًا بالتحدث بنبرة نقدية تجاه الجهة التي يتعاون معها، فتم تحليل سلوكه وربطه بعوامل خارجية (مثل تواصله مع أطراف جديدة) للتأكد من عدم وجود اختراق أو تغيير في الموقف النفسي.

٢. تقديم الدعم اللازم للحفاظ على التعاون.

التعريف: يقصد به تزويد المصدر بالدعم النفسي والاجتماعي والمهني المناسب لظروفه، بما يعزز ولاءه واستمراريته، مثل التقدير المعنوي، المساعدة في حل مشكلاته الشخصية، أو توفير بيئة تواصل آمنة.

مثال: يواجه أحد المصادر ضغوطًا مالية قد تدفعه للتراجع، فيتم تقديم دعم بسيط عبر تغطية احتياجات محددة بطريقة تحفظ كرامته وتزيد من التزامه بالتعاون.

٣. مراقبة مدى التوافق مع المهام المطلوبة.

التعريف: هي عملية تقييم دورية لمدى استمرار توافق قدرات

المصدر واهتماماته مع نوعية المهام المكلف بها، والتأكد من أنـه لا يتعرض للإرهاق أو تجاوز لطاقته النفسية.

مثال: بعد فترة من العمل، يلاحظ الضابط أن المصدر بدأ يظهر علامات ملل أو ضعف تركيز في نوع معين من المهام، فيُعـاد توزيـع مهامه إلى نطاق يناسب شخصيته وقدراته ليبقى فعالًا ومنضبطًا.

الفصل التاسع: أخلاقيات التعامل النفسي والاستخباراتي

١. حدود قانونية واضحة: حماية المصدر وحقوقه.

التعريف: هي مجموعة مـن الضـوابط التـي تضـمن احتـرام القوانين الوطنية والدولية في التعامل مع المصادر، مع التركيز على حماية كرامتهم، خصوصيتهم، وسلامتهم الجسدية والنفسية.

أي نشاط استخباراتي يجب أن يتم ضمن إطار قانوني ومهنـي واضح يمنع الانتهاكات أو الاستغلال.

مثال: عند جمع المعلومات من مصـدر مـدني، يـتم التأكـد من أن المقابلة تُجرى فـي مكـان آمـن ومحايـد، مـع توضـيح أن التعاون يتم طوعًا دون أي تهديد أو ضغط، حفاظًـا علـى سـلامته القانونية والنفسية.

٢. التوازن بين الأمن والإنسانية.

التعريف: يقصد به تحقيق التوازن بين متطلبات الأمن القومي أو المؤسسي وبين الاعتبارات الإنسانية في التعامل مع الأفراد.

الغاية هي الحصول على المعلومات دون الإضرار بالمصدر نفسيًا أو أخلاقيًا، مع الحفاظ على قيم العدالة والاحترام.

مثال: عند ملاحظة أن أحد المصادر يمر بأزمة عائلية، يتم تأجيل المقابلات أو المهام الميدانية مؤقتًا حتى يستعيد توازنه، احترامًا لظروفه الإنسانية رغم أهمية المعلومات.

٣. شفافية الغرض من التقييم

التعريف: تعني أن عملية التقييم النفسي أو السلوكي للمصدر يجب أن تكون ذات هدف واضح ومعلن له بقدر مناسب، بحيث لا يشعر بالخداع أو الاستخدام النفسي المفرط.

تُعد الشفافية الجزئية أحد عوامل بناء الثقة المستدامة بين الضابط والمصدر.

مثال: قبل إجراء اختبار نفسي مختصر، يتم إبلاغ المصدر بأن الغرض هو "فهم أسلوب تعامله مع الضغط الميداني"، دون كشف التفاصيل الفنية للاختبار، وبذلك يُحافظ على الشفافية المهنية.

٤. منع استغلال الضعف أو الإكراه.

التعريف: هو مبدأ أساسي في الأخلاقيات الاستخباراتية يمنع تمامًا استخدام نقـاط الضـعف النفسـي أو الاجتمـاعي للمصـدر كوسيلة للضغط أو الابتزاز.

التعاون يجب أن يكون قائمًـا علـى الاقتنـاع والرضـا الـذاتي وليس الخوف أو الحاجة.

مثال: يُمنع استخدام ملفات شخصـية أو معلومـات حساسـة للضغط على المصدر لتقديم معلومات إضافية، بـل يـتم اللجـوء إلى الحوار والإقناع والتفاهـم لضمان تعاون مستقر وأخلاقي.

الفصل العاشر: دراسات حالة وتطبيقات

الحالة | المصدر | الطريقة | النتيجة|

| --- | ----- | ----- |------|------- |

|باحـث أكـاديمي | HUMINT | تواصـل رسـمي وموافقـة مكتوبة | تقارير تحليلية محايدة|

|منظمـة مدنيـة | OSINT | تحليـل منشـورات وتقـارير | سياسات واقعية لتحسين السلامة|

|بيانات حكومية مفتوحـة | رقميـة | تحليـل مـروري قـانوني | دعم التخطيط الأمني|

الملاحق الاحترافية

١. نموذج تقييم المصدر النفسي والفسلجي.

معايير تقييم الشخصية، الدوافع، السمات الفسلجية.

نقاط تقييم من ٠ إلى ٣ لكل سمة.

تصنيف: منخفض، متوسط، مرتفع مع توصية بالمتابعة أو الانسحاب.

٢. جدول تحليل أنماط الشخصية

السمة	وصف	درجة ٠–٣	ملاحظات
الانضباط	القدرة على الالتزام بالتعليمات		
التحكم بالعاطفة	ضبط الانفعالات		
الصراحة	الصدق والشفافية		
الدافعية	الهدف والاندفاع		

٣. استبيان تحديد الدوافع النفسية للمصدر

أسئلة مقسمة لدوافع مادية، فكرية، انتمائية.

طريقة الإجابة (١-٥) Likert scale: لتقييم مستوى الدافع.

يستخدم لمقارنة السمات والنوايا قبل البدء بالتجنيد أو التعاون.

الخاتمة الكراس يقدم مرجعًا أكاديميًا وتدريبيًا متكاملاً :

يجمع بين التحليل النفسي، الفسلجي، والباراسيكولوجي.

يوفر أدوات تقييم علمية وقابلة للتطبيق العملي.

يراعي الأطر القانونية والأخلاقية.

يمكن استخدامه للتدريس الأكاديمي أو كدليل تـدريبي فـي المؤسسات الأمنية.

الملحق رقم ٣

الكراس التدريبي الاحترافي لاستشراف الأخبار والتوقعات المهنية (نسخة موسعة).

المقدمة

هذا الكراس التدريبي المتكامل مُصمَّم ليجعل المتدرب قادرًا على:

١. تحليل الأخبار بدقة عالية.

٢. فهم الرسائل الخفية.

٣. بناء التوقعات المهنية.

٤. تطبيقها مباشرة في الميدان الأمني والاستخباراتي والنفسي.

أهداف المقدمة

١. توضيح أهمية مهارة استشراف الأخبار والتوقعات.

٢. ربط المعرفة النظرية بالتطبيق العملي.

٣. تحفيز المتدرب على التفكير الاستراتيجي والتحليلي.

تمارين مقترحة

قراءة خبر يومي من وسيلة إعلام مختلفة، تسجيل المؤشـرات الخفية، ومناقشتها مع المجموعة.

تمرين على مقارنة الخبر التحليلي مع الخبر الإخباري المباشر.

الفصل الأول: المفهوم العام لاستشراف الأخبار (الوحدة التأسيسية)

الأهداف التدريبية

١. التمييز بين الخبر، التحليل، والتوقع.

٢. تطوير القدرة على التعرف على المؤشرات المبكرة.

٣. فهم السياق الكامل لكل خبر.

الشرح الموسع

١. تعريـف استشـراف الأخبـار: قـراءة الخبـر ضـمن سـياقه وتحويله إلى تقديرات مستقبلية قابلة للاستخدام.

الفرق بين الخبر والتحليل والتوقع

عناصر الاستشـراف: فهـم السـياق، قـراءة الفـاعلين، تحليـل اللغة، تحديد الدوافع، بناء السيناريوهات.

تمارين عملية

١. تحليل خبر مختصر، تحديد الرسائل الخفية، تقديم تقدير أولي للموقف.

٢. استخدام جدول مقارنة: مصدر الخبر - مصداقية - دافع محتمل أثر محتمل.

الفصل الثاني: مصادر المعلومات وأنواع الأخبار

الأهداف التدريبية

١. تمييز المصادر المفتوحة والمغلقة.

٢. التحقق من مصداقية الأخبار.

٣. تحليل تأثير المصادر على السياق النفسي للخبر.

الشرح الموسع

١. المصادر المفتوحة (OSINT) : وسائل الإعلام، الصحافة الاستقصائية، وسائل التواصل، تقارير مراكز الدراسات.

٢. المصادر المغلقة: تقارير استخباراتية، اتصالات دبلوماسية.

٣. أنواع الأخبار: مباشرة، مركبة، مضللة، منقوصة.

تمارين عملية

١. مقارنة خبر بين ثلاث مصادر مختلفة وتحليل الانحياز والمصداقية.

٢. إنشاء مخطط لتحديد درجة موثوقية المصدر وتأثيره على التحليل.

الفصل الثالث: منهجيات تحليل الأخبار

الأهداف التدريبية

١. تفكيك الخبر وتحليل الرسائل الخفية.

٢. فهم السلوك السابق للجهة الناشرة.

الشرح الموسع

١. تحليل بنية الخبر: العنوان، المتن، الشخصيات، المكان، الوقت.

٢. تحليل الرسائل الخفية: ما لم يُذكر، لغة التعبير، التسلسل.

٣. التحليل السلوكي للجهة الناشرة: توجه الوسيلة، تاريخها، ارتباطاتها، أسلوب التغطية.

تمارين عملية

١. قراءة خبر وتحليل الرسائل المضمرة باستخدام نموذج التحليل النفسي.

٢. تحليل لغة الجسد أو الإيحاءات عند الناشر (إن أمكن).

الفصل الرابع: أدوات استشراف الاتجاهات والتوقعات

الأهداف التدريبية

١. تحويل التحليل إلى توقعات عملية.

٢. استخدام المؤشرات الضعيفة والموجات الإعلامية.

٣. دمج التحليل الكمي والنوعي.

الشرح الموسع

١. نماذج التفكير الاستشرافي: المؤشرات الضعيفة، موجات الإعلام، الاستجابة المتأخرة.

٢. أدوات التحليل الكمي: تحليل التكرار، تحليل الارتباط، رسم منحنيات الزمن.

٣. الأدوات الرقمية: تتبع الترند، تحليل بيانات التواصل، نظم الإنذار المبكر الإعلامي.

تمارين عملية :

١. إنشاء مخطط زمني لتحركات الأخبار الرئيسية في موضوع معين.

٢. استخدام برنامج رقمي لرصد الترندات وتحليل المؤشرات.

الفصل الخامس: بناء التوقعات المهنية

الأهداف التدريبية

١. إصدار تقديرات موقف واقعية.

٢. التمييز بين التوقع القصير، المتوسط، والطويل.

٣. تجنب الأخطاء الشائعة في التوقع.

الشرح الموسع

١. شروط التوقع الجيد: يستند إلى دليل، قابل للاختبار، يصف المسار.

٢. الأخطاء الشائعة: التحيز، تضخيم المؤشرات، الاعتماد على مصدر واحد، إسقاط الرغبات.

تمارين عملية

١. بناء توقع لموقف خلال ٧٢ ساعة باستخدام جميع المؤشرات المتاحة.

٢. تمرين على تقييم النتائج بعد ٢٤ ساعة ومقارنة التوقع بالواقع.

الفصل السادس: السيناريوهات التدريبية الاحترافية

الأهداف التدريبية

١. تدريب المتدرب على التعامل مع أحداث متنوعة.
٢. بناء ردود فعل واستراتيجيات واقعية.

السيناريوهات الموسعة

١. تصعيد عسكري مفاجئ.
٢. إعلان سياسي دولي.
٣. أزمة اقتصادية إقليمية.
٤. حرب نفسية إعلامية موجهة.
٥. تسريب يهدد الأمن الداخلي.
٦. حملة تضليل كبرى.
٧. انهيار إعلامي موجه.
٨. ضغط نفسي على الجمهور.
٩. تمويه إعلامي لإخفاء عملية.
١٠. استخدام الذكاء الاصطناعي لنشر الإيحاءات.

تمارين عملية

تحليل كل سيناريو، تحديد التهديدات، وضع خطة مواجهة، وتقديم تقرير تنفيذي.

الفصل السابع: التطبيقات العملية والتمارين

١. تحليل خبر بخمسة مستويات: المحتوى، اللغة، الدوافع، التوقع الأولي، احتمالات الانعكاس.

٢. مقارنة تغطية خبر بين ثلاث وكالات.

٣. توقع مسار حدث خلال ٧٢ ساعة.

٤. كشف الانحيازات الإدراكية لدى محرّر الخبر.

٥. قياس التأثير النفسي للخبر على الجمهور.

الفصل الثامن: الحرب النفسية الإعلامية

الأهداف التدريبية

١. فهم كيفية استخدام الخبر كسلاح.

٢. تحليل التأثير النفسي للرسائل الإعلامية.

٣. تطوير استراتيجيات مواجهة.

تمارين عملية

تحليل خبر موجه، اكتشاف التلاعب الإدراكي، تقدير التأثير النفسي، ووضع خطة مواجهة.

الفصل التاسع: منظومة الإنذار المبكر الإعلامي

المحتوى

١. المؤشرات الحرجة: التكرار المفاجئ، تغيّر اللغة، ظهور فاعلين جدد.

٢. أدوات الاستشعار المبكر: الرادار الإعلامي، أنظمة مراقبة الترند، التحليل النفسي للخطابات.

٣. إعداد تقارير الإنذار: ملخص تنفيذي، المؤشر، قراءة الاتجاه، التوقع قصير المدى.

الفصل العاشر: دليل الضابط المحترف

١. قواعد التعامل مع الأخبار عالية الخطورة: التثبّت الثلاثي، المقارنة الحتمية، تقييم المرسل.

٢. بروتوكول التفريغ النفسي للخبر: فصل اللغة عن المحتوى، تحليل الإيحاءات، تقدير الضغط النفسي المقصود.

الفصل الحادي عشر: النماذج الجاهزة

١. نموذج تحليل خبر من ٧ مستويات.

٢. نموذج تقدير موقف إعلامي.

٣. نموذج بناء توقع خلال ٧٢ ساعة.

٤. نموذج تحليل حرب نفسية معادية.

الفصل الثاني عشر: السيناريوهات الموسعة

١. حملة تضليل كبرى.

٢. انهيار إعلامي موجه.

٣. تسريب يؤدي لاضطراب أمني.

٤. إشاعة تحشيد سياسي.

٥. خبر كارثي متعمد.

٦. توظيف حادث أمني.

٧. أزمة اقتصادية مفتعلة.

٨. ضغط نفسي على الجمهور.

٩. تمويه إعلامي لإخفاء عملية.

١٠. استخدام الذكاء الاصطناعي لنشر الإيحاءات.

الخاتمة

الكراس هـو مرجـع تـدريبي متكامـل يُمكـن المتـدرب مـن تحويل المعرفة إلى مهارة عملية قابلة للتطبيق في الميدان الأمني، الاســتخباراتي، والتحليلــي النفســي، مــع تمــارين عمليــة، سيناريوهات حقيقية، ونمـاذج جـاهزة، ليصـبح جـاهزًا لإصـدار التوقعات وتحليل الأخبار بشكل مستقل واحترافي.

كراس تخصصي في تطوير المصادر المميزة

المقدمة

تطوير المصادر المميزة

(High-Value Sources Development - HVSD) يُعـد مـن أهم مفاصل العمل الاستخباراتي، كونه يركـز علـى الوصـول إلـى أفراد أو كيانات تمتلك قدرات فريـدة، تـأثير واسـع، أو معلومـات حساسة تُحدث فرقاً في التقييمات الاستراتيجية وصنع القرار.

هذا الكراس يُقدم منهجاً عملياً ومنظماً لتطوير هذه الفئة مـن المصــادر، مــع التركيــز علــى الأدوات، الأســاليب، المراحــل، السيناريوهات، ونماذج التشغيل.

الفصل الأول: المفهوم العام للمصادر المميزة

١. تعريف المصادر المميزة

هي مصادر بشرية أو تقنية تمتلك أحد أو جميع الخصائص التالية:

١. معلومة حساسة أو نادرة يصعب الحصول عليها بطرق أخرى.

٢. قابلية التأثير داخل المؤسسة أو المجال الذي تعمل فيه.

٣. موقع وظيفي أو اجتماعي مهم يسمح بالوصول الدائم للمعلومات.

٤. ارتباطات وشبكات علاقات معقدة تمنح رؤية أعمق للأحداث.

٢. خصائص المصدر المميز

١. قربه من مركز صنع القرار.

٢. قدرته على الوصول المستمر للبيانات.

٣. دوافعه المركبة (أيديولوجية، مادية، نفسية).

٤. سهولة أو صعوبة تجنيده.

٥. مستوى المخاطر المرتبطة به.

٣. الفرق بين المصدر العادي والمصدر المميز

العنصر	المصدر العادي	المصدر المميز

نوع المعلومة | عادية/تكتيكية | حساسة/استراتيجية|

المخاطر | منخفضة | عالية|

إدارة التشغيل | بسيطة | معقدة|

القيمة | متوسطة | عالية جداً|

الفصل الثاني: تصنيفات المصادر المميزة

١. مصادر حساسة داخل المؤسسات

١. مراكز القيادة والسيطرة.

٢. الكادر السياسي.

٣. المسؤولون الماليون.

٤. النووي/العسكري/التقني.

٢. مصادر ضمن القطاع الخاص

١. رجال الأعمال.

٢. شركات التكنولوجيا.

٣. القطاع المالي.

٤. شبكات النقل والاتصالات.

٣. مصادر اجتماعية/نخبوية

١. مؤثرون.

٢. أكاديميون.

٣. مرجعيات اجتماعية.

٤. إعلاميون.

٤. مصادر تقنية متقدمة

١. مصادر إلكترونية (Cyber-HUMINT).

٢. مصادر شبكات التواصل.

٣. مصادر عبر الذكاء الاصطناعي التحليلي.

الفصل الثالث: مراحل تطوير المصدر المميز

١. مرحلة الدراسة الأولية (Profiling)

تشمل:

١. تحليل الخلفية الاجتماعية.

٢. تحليل السلوك.

٣. معرفة الدوافع.

٤. تحديد نقاط الضعف والقوة.

٥. تقييم احتمالية التعاون.

٢. مرحلة الاقتراب والدخول (Access Introduction)

أساليب الاقتراب:

١. المناسبات المهنية.

٢. التواصل غير المباشر عبر وسطاء.

٣. الاهتمام الأكاديمي أو البحثي.

٤. الاحتياجات النفسية للمصدر.

٣. مرحلة بناء الثقة (Trust Building)

تتضمن:

١. درج التواصل.

٢. اختبار الاستجابة.

٣. خلق مبررات طبيعية للاستمرار.

٤. اكتشاف حدود المخاطر.

٤. مرحلة التشغيل الفعلي (Operational Running)

تشمل:

١. تحديد آليات الاتصال.

٢. تحديد نوع المعلومات المطلوبة.

٣. تنظيم السلم الهرمي للمهام.

٤. إدارة الضغوط والمخاطر.

٥. مرحلة التقييم والتحسين (Periodic Review)

١. تقييم قيمة المعلومة.

٢. تقييم تغيّرات سلوك المصدر.

٣. تقييم المخاطر المتصاعدة.

٤. إعادة ضبط العلاقة.

الفصل الرابع: أدوات وأساليب تطوير المصادر

١. الأدوات النفسية

١. بناء الهوية المشتركة.

٢. الإيحاء بالمكانة.

٣. إدارة الاحتياجات العاطفية.

٤. معالجة المخاوف والهواجس.

٢. الأدوات المهنية

١. تقديم منصة مهنية.

٢. تسهيل الظهور والنفوذ.

٣. دعم مشاريع مهنية.

٣. الأدوات المالية

١. الدعم المالي المباشر.

٢. الدعم غير المباشر.

٣. الترتيبات الاقتصادية.

٤. الأدوات العملياتية

١. التقنيات السرية.

٢. الاتصالات المؤمنة.

٣. اللقاءات الدائرية.

الفصل الخامس: معايير اختيار المصدر المميز

المعايير الأساسية

١. القرب من المعلومات.

٢. الاستعداد النفسي.

٣. قابلية التشغيل.

٤. الانضباط.

٥. الاستقرار الوظيفي.

٦. القدرة على النقل الدقيق.

المعايير الثانوية

١. شبكة العلاقات.

٢. طريقة التفكير.

٣. مستوى المخاطر.

الفصل السادس: إدارة تشغيل المصادر المميزة

١. طرق الاتصال

١. لقاء مباشر.

٢. اتصال مؤمن.

٣. وسيط بشري.

٤. قناة مزدوجة (Hybrid Channel) .

٥. طرق غير تقليدية مثل (Dead Drop).

٢. تأمين المصدر

١. إخفاء الهوية.

٢. إجراءات الطوارئ.

٣. خطة الانسحاب.

٤. حماية العائلة.

٣. تأمين الضابط المشغل

١. فصل الملفات.

٢. منع الكشف.

٣. خطط الخداع.

الفصل السابع: المخاطر النموذجية للمصادر المميزة

١. المخاطر الأمنية

١. كشف العلاقة.

٢. مراقبة اتصالات المصدر.

٣. الاختراق المضاد.

٢. المخاطر النفسية

١. التردد.

٢. الشعور بالذنب.

٣. الضغط العائلي.

٣. المخاطر المهنية

١. النقل الوظيفي.

٢. فقدان الوصول للمعلومة.

٣. المخاطر التشغيلية.

٤. انهيار منظومة التواصل.

٥. انحراف المصدر.

الفصل الثامن: نماذج وطرق تقييم أداء المصادر

١. نموذج التقييم الستّي

١. الدقة.

٢. السرعة.

٣. السرية.

٤. القيمة.

٥. الاستمرارية.

٦. المخاطر.

الفصل التاسع: سيناريوهات عملية حديثة لتطوير المصادر

السيناريو ١: تطوير مصدر داخل مؤسسة سيادية

١. خطوات الاقتراب.

٢. دوافع المصدر.

٣. طريقة التشغيل.

٤. التحديات.

٥. النتائج المتوقعة.

السيناريو ٢: تطوير مصدر من القطاع الأكاديمي

١. كيف تبدأ العلاقة عبر مشروع بحثي.

٢. بناء الثقة.

٣. آليات التشغيل الآمنة.

السيناريو ٣: تطوير رجل أعمال مرتبط بدولة معادية

١. استثمار الاحتياجات.

٢. إدارة المخاطر.

٣. استخراج المعلومات التجارية/الاستخباراتية.

السيناريو ٤: تطوير مصدر رقمي (Cyber-HUMINT)

١. الاختراق غير المباشر.

٢. بناء الثقة الرقمية.

٣. تشغيل متقدم عبر الذكاء الاصطناعي.

الفصل العاشر: ملحق النماذج والملفات الجاهزة

١. نموذج دراسة مصدر (Profiling Form) .

٢. نموذج خطة تشغيل مصدر(Operational Plan) .

٣. نموذج خطة اتصال آمن.

٤. نموذج تقييم دوري للمصدر.

٥. نموذج خطة إنهاء آمن (Exit Plan).

الخاتمة

هذا الكراس يمثل إطاراً متكاملاً لتطوير المصادر المميزة ضمن سياق استخباراتي حديث، ويصلح كوثيقة تدريب، أو كمرجع في برامج إعداد الضباط والباحثين في الأمن والاستخبارات.

المحتويات